

STATE OF NORTH CAROLINA Department of Health and Human Services Division of Child and Family Well-Being	REQUEST FOR PROPOSAL NO. 30-25002-DCFW
	Contract Name: Maintenance and Enhancement Services for the Crossroads WIC Management Information System
	Bid Opening Date: Thursday March 6, 2025 at 2PM Eastern
	Issue Date: December 4, 2024
Refer <u>ALL</u> inquiries regarding this RFP to: NC DHHS Office of Procurement, Contracts & Grants (OPCG) Eve.Hens@dhhs.nc.gov	Commodity Code: 432315 – Business Function Specific Software
	Purchasing Agency: Department of Health and Human Services (DHHS)
	Requisition No.: N/A

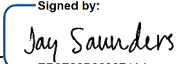
OFFER

The Purchasing Agency solicits offers for Services and/or goods described in this solicitation. All offers and responses received shall be treated as Offers to contract as defined in 9 NCAC 06A.0102(12).

EXECUTION

In compliance with this Request for Proposal (RFP), and subject to all the conditions herein, the undersigned offers and agrees to furnish any or all Services or goods upon which prices are offered, at the price(s) offered herein, within the time specified herein.

Failure to execute/sign offer prior to submittal shall render offer invalid. Late offers are not acceptable.

OFFEROR: Voyatek		
STREET ADDRESS: 9175 Guilford Rd, Suite 218	P.O. BOX:	ZIP: 21046
CITY, STATE & ZIP: Columbia, MD 21046	TELEPHONE NUMBER: 443-276-4788	TOLL FREE TEL. NO
NAME & TITLE OF PERSON SIGNING: Jay Saunders, Vice President	FAX NUMBER:	
AUTHORIZED SIGNATURE:  Signed by: Jay Saunders ED3E96B069674A1...	DATE: 12/17/2025	E-MAIL: jay.saunders@voyatek.com

Offer valid for two hundred seventy (270) days from date of offer opening unless otherwise stated here: ____ days

ACCEPTANCE OF OFFER

If any or all parts of this offer are accepted, an authorized representative of the Department of Health and Human Services (hereafter DHHS) shall affix its signature hereto and any subsequent Request for Best and Final Offer, if issued. Acceptance shall create a contract having an order of precedence as follows: Best and Final Offers, if any, Special terms and conditions specific to this RFP, Specifications of the RFP, the Department of Information Technology Terms and Conditions, and the agreed portion of the awarded Vendor's Offer. A copy of this acceptance will be forwarded to the awarded Vendor(s).

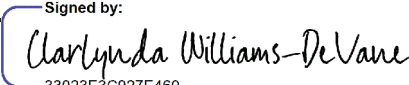
FOR PURCHASING AGENCY USE ONLY	
Offer accepted and contract awarded this date <u>October 7, 2025</u> , as indicated on attached certification,	
by <u>ClarLynda Williams-DeVane</u>	(Authorized representative of DHHS).
 Signed by: ClarLynda Williams-DeVane 33023E3C927E460...	Page 0 of 108

Table of Contents

1.0	ANTICIPATED Procurement Schedule	3
2.0	Purpose of RFP.....	4
2.1	Introduction.....	4
2.2	Agency Background.....	4
2.3	SUMMARY OF PROBLEM Statement.....	7
2.4	Contract Term.....	7
2.5	Effective Date	7
2.6	Contract Type	8
3.0	RFP requirements and Specifications	8
3.1	General requirements and Specifications	8
3.2	Security Specifications.....	9
3.3	Enterprise Specifications	9
3.3.2	SOLUTION ROADMAP (RESERVED).....	10
3.3.3	IDENTITY AND ACCESS MANAGEMENT	10
3.3.4	INTEGRATION APPROACH (RESERVED).....	10
3.3.5	DISASTER RECOVERY AND BUSINESS CONTINUITY (RESERVED).....	10
3.3.6	DATA MIGRATION (RESERVED).....	10
3.3.7	APPLICATION MANAGEMENT (RESERVED)	10
3.3.8	ACCESSIBILITY (RESERVED).....	10
3.4	Business and Technical Requirements.....	10
3.5	Business and Technical Specifications.....	15
4.0	Cost of Vendor's Offer.....	56
4.1	Offer Costs	56
4.2	Payment Schedule.....	56
5.0	Evaluation	57
5.1	Source Selection.....	57
5.2	Evaluation Criteria	58
5.3	Best and Final Offers (BAFO).....	58
5.4	POSSESSION AND REVIEW	58
6.0	Vendor Information and Instructions	58
6.1	General Conditions of Offer	58
6.2	General Instructions for Vendor	60
6.3	Instructions for Offer Submission.....	62
7.0	Other Requirements and Special Terms	64
7.1	Vendor Utilization Of Workers Outside of U.S.	64
7.2	Financial Statements	64
7.3	Financial Resources Assessment, Quality Assurance, Performance and Reliability	65
7.4	Vendor's License or Support Agreements	65
7.5	Resellers (RESERVED).....	65
7.6	DISCLOSURE OF LITIGATION.....	65
7.7	CRIMINAL CONVICTION	66
7.8	Security and Background Checks.....	66
7.9	Assurances.....	66

7.10 Confidentiality of offers	66
7.11 Project Management	67
7.12 Meetings.....	67
7.13 Recycling and Source Reduction	67
7.14 Special Terms and Conditions.....	67
7.15 AGENCY Terms and Conditions (RESERVED)	68
Attachment A: Definitions.....	69
Attachment B: Department of Information Technology Terms and Conditions FOR VENDOR HOSTED SOLUTIONS	73
Attachment C: Description of Offeror	95
Attachment D: Cost Form.....	97
Attachment E: Vendor Certification Form.....	101
Attachment F: Location of Workers Utilized by Vendor.....	102
Attachment G: References.....	103
Attachment H: Financial Review Form.....	104
Attachment K. Federal and Other State Specifications	106

1.0 ANTICIPATED PROCUREMENT SCHEDULE

The Agency Procurement Agent will make every effort to adhere to the following schedule:

Action	Responsibility	Date
RFP Issued	Agency	12/4/24
Written Questions Deadline	Potential Vendors	1/6/25 by 2:00 PM Eastern
Agency's Response to Written Questions/ RFP Addendum Issued	Agency	1/29/25
Offer Opening Deadline	Vendor(s)	3/6/25 by 2:00 PM Eastern
Offer Evaluation	Agency	3/10/25-4/17/25
Selection of Finalists	Agency	4/21/25
Negotiations with Finalists	Agency designees and selected Vendor(s)	5/12/25
Best and Final Offers Deadline from Finalists	Selected Vendors	6/2/25
Contract Award	Agency	8/1/25
Protest Deadline	Responding Vendors	15 days after award

2.0 PURPOSE OF RFP

2.1 INTRODUCTION

The purpose of this RFP and any resulting contract award is to solicit offers for services of a qualified Vendor (hereinafter referred to as the “Vendor”) to provide Crossroads Management Information System (MIS) Maintenance and Enhancement Services (M&E) for the Supplemental Nutrition Program for Women, Infants, and Children (WIC) for the State of North Carolina (State). The M&E services also include rehosting to a cloud environment, defect correction, change order implementation, and production help desk support.

This request is for a close-ended contract between the awarded Vendor and the State to furnish services meeting the specifications and requirements described in this RFP during a specified period, for support of all Crossroads application code and sub-code modules needed to keep the MIS viable and compatible with infrastructure and platform components.

2.2 AGENCY BACKGROUND

The mission of the United States Department of Agriculture Food and Nutrition Service (USDA/FNS), Special Supplemental Nutrition Program for Women, Infants, and Children (WIC) is to safeguard the health of low-income pregnant, postpartum and breastfeeding women, infants, and children up to age five who are at nutritional risk by providing nutritious foods to supplement diets, information on healthy eating, and referrals to health care. WIC is funded by a Federal grant program and is available in all 50 States, 35 Indian Tribal Organizations (ITOs), American Samoa, District of Columbia, Guam, Puerto Rico, the Virgin Islands and the Commonwealth of Northern Mariana Islands.

The North Carolina WIC Program is administered by the Department of Health and Human Services, Division of Child and Family Well-Being. WIC services are provided at Local Health Agencies at clinic sites throughout the state. Clinic Staff are comprised of Competent Professional Authorities (CPA), Registered Dietitians, Lab Technicians, Breastfeeding Peer Counselors, in addition to WIC Program Managers and Coordinators. These staff provide direct WIC participant services including scheduling clients, determining client eligibility, completing nutrition assessment and education, breastfeeding support, and issuing food benefits through the Crossroads Management Information System (MIS). WIC food benefits are redeemed at authorized WIC retailers statewide using the state-issued eWIC card.

In 1984, the United States Department of Agriculture – Food and Nutrition Services (USDA/FNS) requested that the NC WIC Program provide data processing services to assist the Eastern Band of Cherokee Indians (EBCI) WIC to operate an independent program yet have similar features as the NC WIC Program. Since that time, the Eastern Bank of Cherokee Indians has utilized our system and NC will continue to include them in our MIS and eWIC systems.

2.2.1 Crossroads WIC MIS Background

The Crossroads Consortium was created in 2005 in response to the FNS State Agency Model (SAM) mandate for designing, building, and implementing new WIC management information systems (MIS) nationwide. The USDA/FNS produced the SAMs in order to create economies of scale by combining information technology development efforts with multiple states rather than the USDA/FNS funding multiple MIS projects individually. The Crossroads Consortium, with North Carolina as the lead state, awarded a contract to the incumbent vendor Computer Sciences Corporation (CSC) in 2009 to build a SAM system for the states of Alabama, North Carolina, Virginia, and West Virginia. Rollout of the Crossroads SAM system was completed in all four (4) Crossroads Consortium states by 2014, with the North Carolina instance of Crossroads being hosted by the NC Department of Information Technology. In 2017, North Carolina amended the Crossroads contract with CSC to continue providing Maintenance and

Enhancement Services using source code and documentation independent of the other three Consortium states. The Crossroads M&E contract was awarded to the current incumbent Voyatek (formerly known as Three Sigma Software / GCOM) in 2019. These continued M&E services include defect correction, change order implementation, software installation services, and production help desk support.

2.2.2 Subprograms of WIC Program

While the Farmers' Market Nutrition Program (FMNP) and the Breastfeeding Peer Counseling Program (BFPC) are subprograms of the federal WIC Program, every state does not administer these programs. North Carolina does administer these programs, so its instance of the Crossroads source code does include the respective functionality that supports both subprograms.

A description of the State's NC WIC and FMNP program data is included below. The summary provided outlines the State's participation levels, number of users, number of retailers, and peer group structure.

2.2.3 Crossroads Current State-Hosted System Environments and Architecture

The Crossroads solution currently utilizes two different technologies for its applications. The Clinic and State Office applications utilize a .NET Framework Visual Basic Windows Presentation Foundation (WPF) desktop application, the retail Vendor portal website is based on ASP.NET, and the Telehealth participant portal website is based on ASP.NET. All technologies are deployed similarly; the code is deployed on the web server and IIS is configured to allow access to the files. Services are deployed on the application servers and web servers as appropriate.

The main difference between the WPF and ASP.NET technologies is that the WPF is downloaded using ClickOnce technology and executes on the client machine. In the ASP.NET applications, the actual code is executed on the Crossroads web and application servers based on requests from the client. Only a small amount of client code is executed on the client machine, and it is typically related to user interface and service calls rather than business rule execution. All technologies will utilize the application servers to execute service calls. The application servers, which reside in the internal (or system) demilitarized zone (DMZ), will access the database. This ensures that no server in the public-facing web DMZ has direct access to the database.

The client machine requires the Microsoft .NET 4.8 Framework to run the WPF application. The .NET Framework is included as part of Windows 10 and Windows 11. The general flow or process of communication is that all Crossroads WIC personal computers (PC) or desktops/laptops will communicate with the Web server via an intranet or Internet connection. Existing WAN infrastructure can be used along with a local Internet service provider, or other varieties of connectivity that the North Carolina Local Agencies find most compatible with their current infrastructure. Since there is only one centralized database, all transactions are immediately seen by all users for their individual agency if the user has appropriate access rights.

At the close of business each day, the End of Day (EOD) processing is performed on the centrally located Process / Batch Server. This EOD process performs all nightly batch processing and prepares the system for the next day's activities. In order to allow round-robin load balancing, all service requests are stateless. In other words, Crossroads does not maintain session information across individual PC to Server transactions. Any request can be executed on any available server without regard to previous or future requests from the same instance of the application.

All North Carolina WIC clinics and State office operate in the Eastern Standard Time (EST) zone. All areas observe Daylight Saving Time (EDT). No NC local agencies deviate from these time zones.

2.2.4 Web Server for current State-Hosted Solutions

The Web Server provides the “storefront” for all Crossroads WIC PCs. All transactions are submitted to the web server which in turn interacts with the application server, which in turn interacts with the database server. Crossroads uses Microsoft’s IIS 10 or higher to host the centralized .NET Web services. The interaction with the web and application servers will use industry standard XML-based Web Services encrypted via a Secure Sockets Layer (SSL) connection to provide web-enabled, cross-platform independent interfaces to each of the Crossroads WIC PCs. The Central Processing Site will utilize a web farm with a number of servers proportionate to the number of concurrent workstation users. The connection from the web server to the application server will be conducted through a customized IIS http handler. In this case, the web server will act as a proxy to pass through the requests and responses to/from the application.

2.2.5 Application Server for current State-Hosted Solutions

As State Information Technology (IT) standards disallow direct communication between web servers and the database, the application server processes the request from the web server to the database server. Crossroads will use Microsoft’s IIS 10 or higher to host the centralized .NET Web services. The Central Processing Site will utilize a Web farm with a number of servers proportionate to the number of concurrent workstation users. IP load balancing is a hardware-based solution that works well with the proposed software architecture since a stateless Web Server is utilized.

2.2.6 Microsoft SQL Server Failover Cluster Database Servers for current State-Hosted Solutions

The database servers are configured in a Microsoft SQL Server 2016 failover cluster. The production database file itself is approximately 700 GB in size. The online transaction processing database is primary on node 1 of the database cluster. The report database is primary on node 2 of the database cluster in a separate named instance. State staff use Microsoft SQL Server Management Studio (SSMS) to execute queries and other scripting against the database.

2.2.7 Storage Area Network (SAN) for current State-Hosted Solutions

Shared storage is utilized by the production and non-prod servers for various processing purposes, plus for long-term retention of artifacts such as uploaded scanned images and other documentation. For all Crossroads environments, the State is currently using twelve (12) terabytes of a total SAN solution of twenty-seven (27) terabytes.

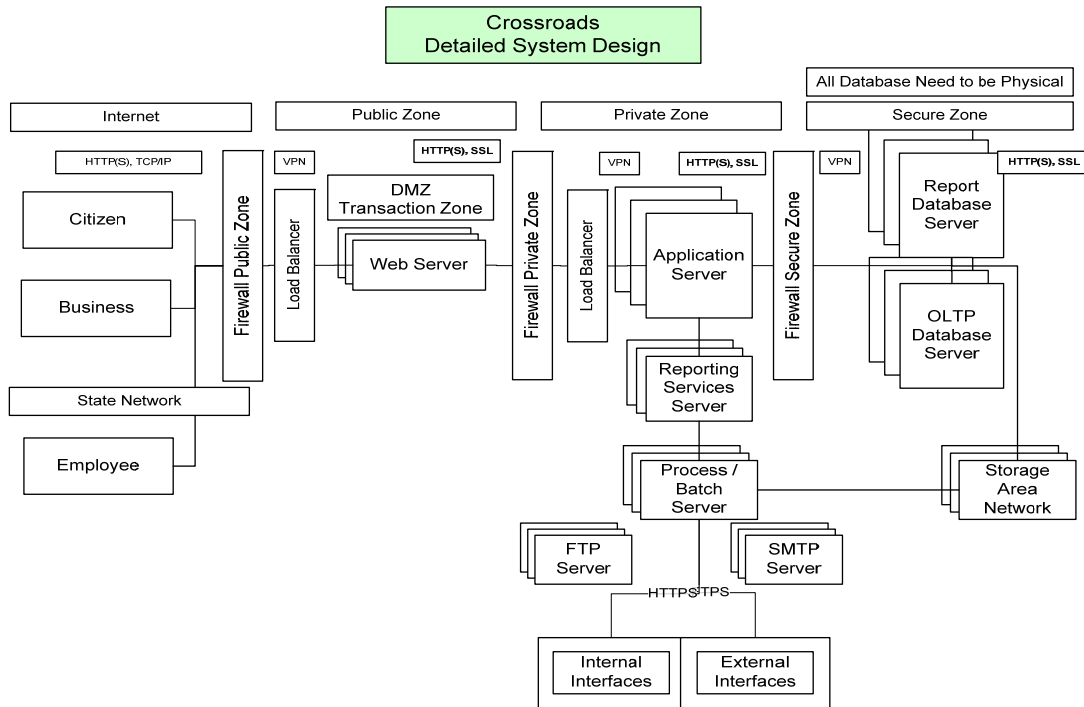
2.2.8 Microsoft SQL Server Reporting Services Server for current State-Hosted Solutions

The Reporting Services Server receives requests from the Crossroads web servers and provides completed reports to the requesting application. This interaction uses industry standard XML-based Web Services encrypted via an SSL connection to provide Web enabled cross platform independent interfaces to each of the Crossroads WIC PCs. The SQL Server Reporting Services standard databases (Report Server and Report Server Temp DB) are hosted on the Reporting Services Server.

2.2.9 Production and Non-Prod Environments

The State currently utilizes one (1) Production environment and five (5) non-Prod environments, made up of a total of approximately sixty (60) servers. The incumbent vendor utilizes an Octopus Deploy solution to maintain software deployments on these servers.

2.2.10 Illustration of current State-Hosted Crossroads System Design



2.3 SUMMARY OF PROBLEM STATEMENT

In addition to providing Maintenance and Enhancement Services (M&E), this RFP solicits offers that rehost (or “lift and shift”) the existing production and non-production Crossroads applications and data from the current State hosted infrastructure to a Vendor managed cloud infrastructure during the eight (8) month Transition-In phase. This approach alleviates the need for the Vendor to provide M&E services on the State-hosted versions of the Crossroads solutions during the M&E Phase. State personnel will continue to have unimpeded access and read-only permissions to the production and non-prod databases in the Vendor managed cloud infrastructure.

2.4 CONTRACT TERM

A contract awarded pursuant to this RFP shall have an effective date as provided in the Notice of Award. The term shall be **seven (7) years** and will expire upon the anniversary date of the effective date unless otherwise stated in the Notice of Award, or unless terminated earlier. The State retains the option to extend the Agreement for **three (3) additional one (1) year** periods at its sole discretion.

2.5 EFFECTIVE DATE

This solicitation, including any Exhibits, or any resulting contract or amendment shall not become effective nor bind the State until the appropriate State purchasing authority/official or Agency official has signed the document(s), contract or amendment; the effective award date has been completed on the document(s), by the State purchasing official, and that date has arrived or passed. The State shall not be responsible for reimbursing the Vendor for goods provided nor Services rendered prior to the appropriate signatures and the

arrival of the effective date of the Agreement. No contract shall be binding on the State until an encumbrance of funds has been made for payment of the sums due under the Agreement.

2.6 CONTRACT TYPE

Definite Quantity Contract - This request is for a close-ended contract between the awarded Vendor and the State to furnish services meeting the specifications and requirements described in this RFP during a specified period of time,

The State reserves the right to make partial, progressive or multiple awards where it is advantageous to award separately by items; where more than one supplier is needed to provide the contemplated specifications as to quantity, quality, delivery, service, geographical areas; or where other factors are deemed to be necessary or proper to the purchase in question.

3.0 RFP REQUIREMENTS AND SPECIFICATIONS

3.1 GENERAL REQUIREMENTS AND SPECIFICATIONS

3.1.1 REQUIREMENTS

Requirement means, as used herein, a function, feature, or performance that the system must provide. If the offer cannot meet the requirements, they will not be evaluated.

3.1.2 SPECIFICATIONS

Specification means, as used herein, a detailed description that documents the function and performance of a system or system component.

The apparent silence of the specifications as to any detail, or the apparent omission of detailed description concerning any point, shall be regarded as meaning that only the best commercial practice is to prevail and that only processes, configurations, materials and workmanship of the first quality may be used. Upon any notice of noncompliance provided by the State, Vendor shall supply proof of compliance with the specifications. Vendor must provide written notice of its intent to deliver alternate or substitute Services, products, goods or other Deliverables. Alternate or substitute Services, products, goods or Deliverables may be accepted or rejected in the sole discretion of the State; and any such alternates or substitutes must be accompanied by Vendor's certification and evidence satisfactory to the State that the function, characteristics, performance and endurance will be equal or superior to the original Deliverables specified.

3.1.3 SITE AND SYSTEM PREPARATION

Vendors shall provide the Purchasing State Agency complete site requirement specifications for the Deliverables, if any. These specifications shall ensure that the Deliverables to be installed or implemented shall operate properly and efficiently within the site and system environment. Any alterations or modification in site preparation, which are directly attributable to incomplete or erroneous specifications provided by the Vendor and which would involve additional expenses to the State, shall be made at the expense of the Vendor.

3.1.4 EQUIVALENT ITEMS

Whenever a material, article or piece of equipment is identified in the specification(s) by reference to a manufacturer's or Vendor's name, trade name, catalog number or similar identifier, it is intended to establish a standard for determining substantial conformity during evaluation, unless otherwise specifically stated as a brand specific requirement (no substitute items will be allowed). Any material, article or piece of equipment of other manufacturers or Vendors shall perform to the standard of the item named. Equivalent offers must be accompanied by sufficient descriptive literature and/or specifications to provide for detailed comparison.

3.1.5 ENTERPRISE LICENSING

In offering the best value to the State, Vendors are encouraged to leverage the State's existing resources and license agreements, which can be viewed here:

<https://it.nc.gov/resources/statewide-it-procurement/statewide-it-contracts>

- a) Identify components or products that are needed for your solution that may not be available with the State's existing license agreement.
- b) Identify and explain any components that are missing from the State's existing license agreement.
- c) If the Vendor can provide a more cost effective licensing agreement, please explain in detail the agreement and how it would benefit the State.

3.2 SECURITY SPECIFICATIONS

3.2.1 SOLUTIONS HOSTED ON STATE INFRASTRUCTURE (RESERVED)

3.2.2 SOLUTIONS NOT HOSTED ON STATE INFRASTRUCTURE

The Crossroads WIC MIS will be required to receive and securely manage data that is classified as Restricted. Refer to the North Carolina Statewide Data Classification and Handling policy for more information regarding data classification. The policy is located at the following website: <https://it.nc.gov/document/statewide-data-classification-and-handling-policy>.

To comply with the State's Security Standards and Policies, State agencies are required to perform annual security/risk assessments on their information systems using NIST 800-53 controls. This requirement additionally applies to all Vendor-provided, agency-managed Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) solutions which will handle data classified as Medium Risk (Restricted) or High Risk (Highly Restricted) data.

(a) Vendors shall provide a completed Vendor Readiness Assessment Report Non-State Hosted Solutions ("VRAR") at offer submission. This report is located at the following website: <https://it.nc.gov/documents/vendor-readiness-assessment-report>

(b) Upon request, Vendors shall provide a current independent 3rd party assessment report in accordance with the following subparagraphs (i)-(iii) prior to contract award. However, Vendors are encouraged to provide a current independent 3rd party assessment report in accordance with subparagraphs (i)-(iii) at the time of offer submission.

(i) Federal Risk and Authorization Management Program (FedRAMP) certification, SOC 2 Type 2, ISO 27001, or HITRUST are the preferred assessment reports for any Vendor solutions which will handle data classified as Medium Risk (Restricted) or High Risk (Highly Restricted).

(ii) Reserved.

(iii) An IaaS vendor cannot provide a certification or assessment report for a SaaS provider UNLESS permitted by the terms of a written agreement between the two vendors and the scope of the IaaS certification or assessment report clearly includes the SaaS solution.

(c) Additional Security Documentation. Prior to contract award, the State may in its discretion require the Vendor to provide additional security documentation, including but not limited to vulnerability assessment reports and penetration test reports. The awarded Vendor and any subcontractors of the awarded Vendor shall provide such additional security documentation upon request by the State during the term of the contract.

3.3 ENTERPRISE SPECIFICATIONS

3.3.1 ARCHITECTURE DIAGRAMS

The two diagrams are Network Architecture and Technology Stack. The State utilizes architectural diagrams to better understand the design and technologies of a proposed solution. Details on these diagrams can be found at the following link: <https://it.nc.gov/resources/statewide-it-procurement/vendor-engagement-resources#Tab-Architecture-1192>

The provision of these two diagrams is a requirement at offer submission. If they are not supplied at that time, the Vendor's offer will be considered non-responsive and will not be evaluated.

There may be additional architectural diagrams requested of the vendor after contract award, at no additional cost. This will be communicated to the vendor by the agency as needed during the project.

An example of the current State-Hosted Crossroads design is illustrated above in Section 2.2 Agency Background, , subsection 2.2.10 Illustration of current State-Hosted Crossroads System Design.

3.3.2 SOLUTION ROADMAP (RESERVED)

3.3.3 IDENTITY AND ACCESS MANAGEMENT

The proposed solution must externalize identity and access management. The protocols describing the State's Identity and Access Management can be found at the following link: <https://it.nc.gov/services/vendor-engagement-resources#Tab-IdentityAccessManagement-1241>

Describe how your solution supports the above protocols, as well as making them available for application integration/consumption.

3.3.4 INTEGRATION APPROACH (RESERVED)

3.3.5 DISASTER RECOVERY AND BUSINESS CONTINUITY (RESERVED)

3.3.6 DATA MIGRATION (RESERVED)

3.3.7 APPLICATION MANAGEMENT (RESERVED)

3.3.8 ACCESSIBILITY (RESERVED)

3.3.9 ENTERPRISE, SERVICES, AND STANDARDS

Vendors should refer to the Vendor Resources Page for information on North Carolina Department of Information Technology regarding architecture, security, strategy, data, digital, identity and access management and other general information on doing business with state IT process.

The Vendor Resources Page found at the following link: <https://it.nc.gov/vendor-engagement-resources>. This site provides vendors with statewide information and links referenced throughout the RFP document. Agencies may request additional information.

3.4 BUSINESS AND TECHNICAL REQUIREMENTS

This RFP seeks to obtain a Vendor to provide maintenance and enhancement services of the North Carolina Crossroads WIC Management Information System, including system cloud hosting, in accordance with the Service Level Agreement and other technical specifications. Vendor must address each requirement listed within this Section 3.4 within their proposal to confirm that the proposed solution meets the requirements within this RFP.

3.4.1 SYSTEM

- a) Confirm that the State will retain all ownership rights to the Crossroads source code and its derivative works.
- b) The State will not consider offers for an alternative replacement MIS system, nor consider offers to convert the State's Crossroads ownership rights to a Software as a Service (SaaS) solution. Confirm that Vendor solution is not an alternate replacement MIS system and that Vendor will not convert Crossroads ownership rights to a SaaS solution.

- c) Confirm that Vendor will not impose any “black out periods” on any M&E activity, nor allow Vendor efforts with other state agencies to introduce delays or other impacts on execution of this contract.

3.4.2 OTHER MAINTENANCE TASKS

The following requirements govern this product and the related technical specifications. Vendor will indicate compliance with each requirement within **Table 3.4.2** located below.

a) Interface with Existing or Future WIC Electronic Benefits Transfer (WIC EBT)

Crossroads is required to interface with the current or any future WIC EBT provider. As of the date of this RFP, the Crossroads system is only compatible with the interim version of the WIC Universal MIS-EBT Interface (WUMEI) from July 2013. The system is scheduled for an upgrade to support the latest WUMEI by March 2026.

1. Should the upgrade to the latest WUMEI specification not be completed prior to the March 2026 deadline, planning will commence by the State, the WIC EBT Provider, and the Vendor to complete the upgrade the Crossroads production system to the new WUMEI as well as any related technology changes at no additional cost. All planning, JAD sessions, development, testing, support for UAT, pilot and rollout related to the WUMEI will be performed by the Vendor. The production upgrade completion date will be solely determined by the State.
2. Should Crossroads contain an interface to a non-State owned or licensed software component required to support the WUMEI interface, the Vendor must maintain or substitute such component to ensure no interruption in EBT processing.

b) Correction of Unknown Defects or Issues Introduced Prior To Contract Execution

Vendor must correct any unknown defects or issues in the Crossroads system that originated prior to work by the Awarded Vendor, using the defect correction process and at no additional cost to the State. All defects known prior to the award of this Contract will be classified as adaptive changes and addressed by the Awarded Vendor using the Maintenance Change Request process.

c) Maintenance Change Requests and Data Corrections

The Vendor must perform all application maintenance, which refers to routine support activities that include corrective, adaptive, and perfective changes.

1. Corrective changes are tasks to correct errors or deficiencies in the Crossroads system, at no additional cost to the State
2. Adaptive changes are revisions to the Crossroads system to meet the changing WIC, State Agency, or USDA/FNS policy, statutory, security, or regulatory requirements, and will use the change management process and Supplemental Service Hours;
3. Perfective changes are improvements to the Crossroads system so that it will perform in a more efficient, economical, and/or effective manner, at no additional cost to the State

Corrective and perfective application maintenance examples can include activities such as revising standard or state-created ad-hoc reports, creating new reports or data extracts (CSV or similar formats at the sole discretion of the State), creating (and executing at the request of the State) data scripts to implement limited data correction changes regardless of root cause, and making limited performance alterations or minor improvements to imbedded passwords, data input and display screen designs and layouts.

State personnel will also be granted read-only access to the cloud computing platforms at no additional cost, to exercise data reporting, or other queries against the Production and non-Production environments at the sole discretion of the State.

d) Other FNS Programs Covered by this RFP

The Farmers' Market Nutrition Program (FMNP) and the Breastfeeding Peer Counseling Program (BFPC) functionality are also components of the North Carolina Crossroads system and are covered by all M&E processes throughout this RFP.

Table for 3.4.2 Other Maintenance Tasks

Does the Vendor meet the requirements listed above?	yes	no
a) Interface with Existing or Future WIC Electronic Benefits Transfer (WIC EBT)		
b) Correction of Unknown Defects or Issues Introduced Prior To Contract Execution		
c) Maintenance Change Requests and Data Corrections		
d) Other FNS Programs Covered by this RFP		

3.4.3 PRODUCT DELIVERABLES

- a) The Vendor's proposed schedule for the provision of product deliverables and documentation for review and approval by North Carolina WIC must adhere to the dates specified in Table 1 below. Electronic copies of the draft and final documentation and deliverables will be supplied to the State through use of a secure electronic documentation repository, hosted and managed by the Vendor. Electronic copies will be provided in Microsoft Office 365 format, unless otherwise specified within this solicitation.
- b) State comments will be provided to the Vendor within ten (10) Business Days of the receipt of draft deliverables. Within five (5) Business Days of receipt of State comments, and after incorporating such comments, the draft of the documentation will be delivered to the State. The State desires to keep deliverable review and revision cycles to a minimum. The above process will be repeated until the State has approved the deliverable in writing. Acceptance by the State will be in the form of a written acknowledgement that the Deliverable meets the specifications as specified in this RFP.
- c) The Vendor will update and maintain product deliverables and documentation for the duration of the Contract, at no additional cost to the State. The approved deliverables and documentation will be updated to reflect changes in system design or operations or as requested by the State. The timing for product deliverables and documentation updates will be determined as part of each change request and each major release.

Deliverables requiring periodic updates will be submitted per the document update schedules included in the description of each deliverable in the associated sections of this RFP.

- d) Timelines for the submission of deliverables are provided in Table 1 below. Details as to what will be in each deliverable are provided in subsequent sections. The Vendor will submit the following deliverables within the timeframe listed for each deliverable in Table 1, or as otherwise specified in this RFP. If preferred, the Vendor may include each of these deliverables in the Appendices section of its proposal bid (after Attachments) and will label each of the deliverables that are requested with the bid proposal as indicated in the "RFP Response Deliverable Label" column in Table 1. These appendices are the agency's preference, but not a requirement.
- e) Deliverables must be itemized under Attachment D in order to receive payment. Deliverables not itemized under Attachment D are at no additional cost.

Table 1 – List of Product Deliverables

Deliverable ID	Deliverable Name	Deliverable Timeline	RFP Response Deliverable Label
1	Transition-In Plan	Described in bid response proposal	Appendix A: Transition-In Plan
2	Product Management Plan	Describe in bid response proposal	Appendix B: Product Management Plan

3A	Product Work Plan and Schedule DRAFT	Describe in bid response proposal	Appendix C: Product Work Plan and Schedule DRAFT
3B	Product Work Plan and Schedule FINAL	During Transition-In – 45 Calendar Days after Contract execution date	
4	Quality Assurance Management Plan	Describe in bid response proposal	Appendix D: Quality Assurance Management Plan
5	Communication and Coordination Plan	Describe in bid response proposal	Appendix P: Communication and Coordination Plan
6	Maintenance and Enhancement Status Reports	Monthly during the life of the contract, aligned with monthly invoice	
7	UAT Readiness Reports	14 Calendar Days Prior to each UAT Start	
8	UAT Completion Reports and System Documentation	21 Calendar Days prior to each Deployment	
9	Production Deployment Plan	During Transition-In: 90 Calendar Days prior to the first statewide deployment	
10	Disaster Recovery and Contingency Plan	Describe in bid response proposal	Appendix F: Disaster Recovery and Contingency Plan
11	Security and Vulnerability Plan	Describe in bid response proposal	Appendix G: Security and Vulnerability Plan
12	Risks and Issues Management Plan	Describe in bid response proposal	Appendix H: Risks and Issues Management Plan
13	Configuration Management / Release Management Plan	Describe in bid response proposal	Appendix J: Configuration Management / Release Management Plan
14	Evidence of Vendor and financial stability (See Section 7 for acceptable documentation)	Describe in bid response proposal	Appendix K: Evidence of Vendor Financial Stability
15	Transition-Out Plan	Describe in bid response proposal	Appendix L: Transition-Out Plan

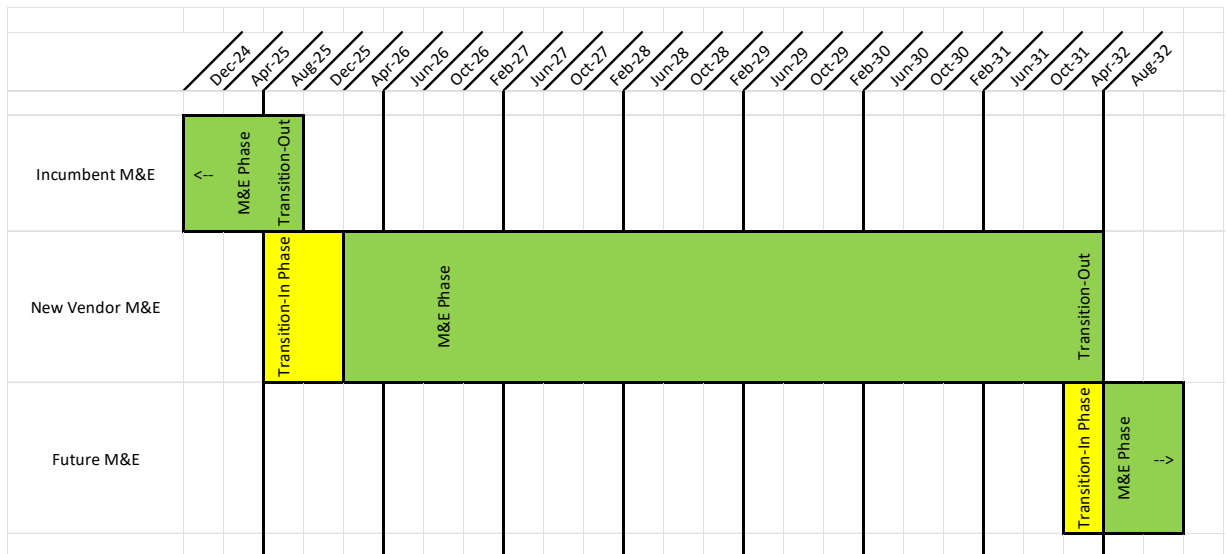
16	Transition-Out Completion Report	During Transition-Out: 10 Calendar Days prior to Contract termination or expiration	
17	Partnerships and Contractual Relationships	Describe in bid response proposal	Appendix M: Partnerships and Contractual Relationships
18	Risk and Security Assessment of Vendor critical systems and infrastructure	Assessment due during the Transition-In Phase.	
19	Help Desk Plan	Describe in bid response proposal	Appendix N: Help Desk Plan
20	Rehosting Implementation and Rollout Plan	Describe in bid proposal	Appendix E: Rehosting Implementation and Rollout Plan
21	Vendor-Hosting Status Report	Monthly during the life of the contract, aligned with monthly invoice	

3.5 BUSINESS AND TECHNICAL SPECIFICATIONS

Please describe your proposed approach to meet all specifications, including capabilities, features, and limitations. All pricing and cost information will be restricted to the Pricing Section of the Vendor's response.

3.5.1 SCOPE

The scope of this RFP includes two phases, the Transition-In Phase and the Maintenance and Enhancement Phase, as illustrated here with tentative dates that are subject to change.



a) Phase I: Transition-In Phase

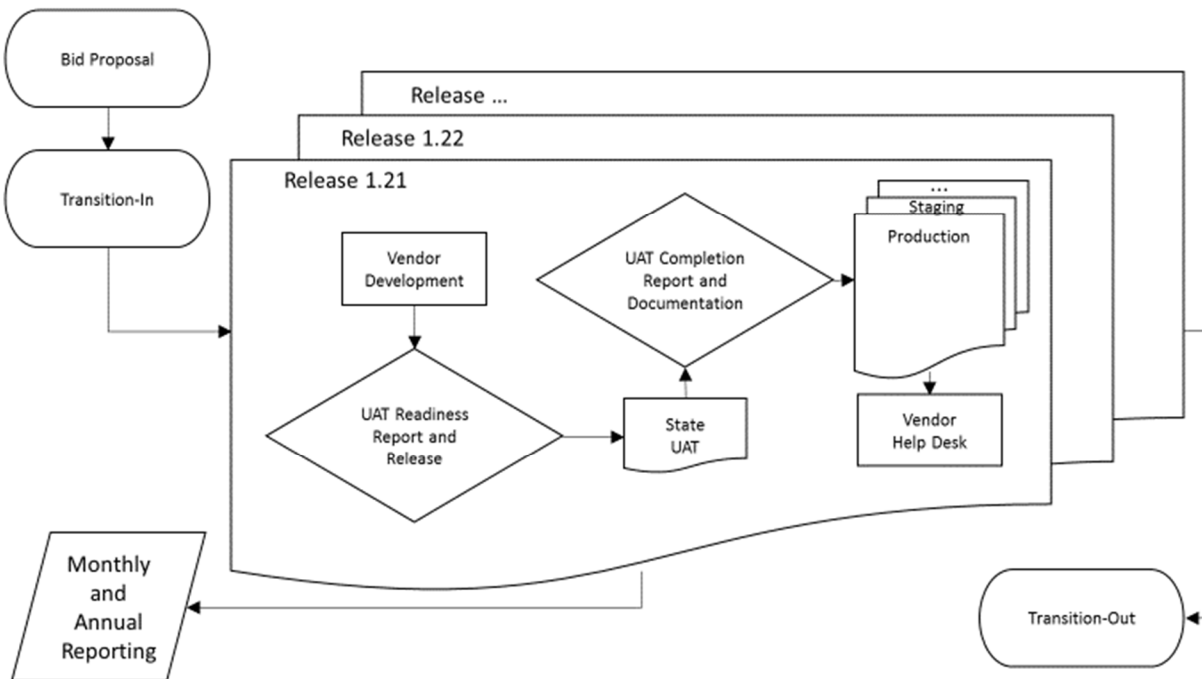
Using the parameters below, describe Vendor's approach to implement the transition-in phase:

1. Expected Phase Timeframe: eight (8) months in duration after Contract Execution
2. The Transition-In Phase is expected to begin immediately after Contract award) and last until either the Maintenance and Enhancement Phase begins or until the existing contract with the incumbent vendor ends. ("Transition-In Phase End Event"), whichever Transition-In Phase End Event occurs first.
3. At the initiation of the Transition-In Phase, the Vendor and the State should meet during the Kick-Off Meeting to discuss and prepare for the completion of Transition-In Phase tasks.
4. Vendor should include a Monthly Transition-In Phase Fee for performing the Transition-In Phase tasks outlined in this RFP.

b) Phase II: Maintenance and Enhancement Phase

Following the Transition-In period, the core concept of the Contract is for the Vendor to provide development, UAT, deployment, and ongoing Help Desk support of multiple iterative releases of the Crossroads system over the life of the Contract as shown below.

Figure 1 - Contract Production Concept



During the Maintenance and Enhancement Phase, the Vendor is expected to provide full Maintenance and Enhancement Services support for Crossroads, independent of the incumbent vendor.

The Maintenance and Enhancement Phase is expected to start on the first Calendar Day after the Transition-In Phase End Event occurs. The Vendor will be expected to perform tasks and deliverables included under Scope of Work, Technical Specifications, and Attachment K.

1. Explain the Vendor's process, either an agile/waterfall hybrid for the State to receive a minimum of three (3) major releases per year, or an agile continuous delivery approach that aligns with the States' business needs and resources.
2. Describe the Vendor's approach in providing a minimum number Change Requests and defect corrections, as provided by the State in each quarter. This approach will ensure that the business needs of the State across the clinic, retail vendor, financial, and related components of Crossroads are being addressed per quarter.

3. Explain how the Vendor maintains and trains appropriate development and test staff to address the breadth of clinic, retail vendor, financial, and related components potentially affected in each major release.
4. Describe Vendor's Rehosting Implementation and Rollout Plan.(Note: If preferred, you may attach a Plan instead. An attached plan is the agency's preference, but not a requirement.) Include in this description, the Vendor's approach in rehosting the State hosted Crossroads solution to a Vendor managed cloud infrastructure prior to the start of the Maintenance and Enhancement phase and address details on the proposed 3rd party cloud computing provider, and the service model proposed between the Vendor and the cloud provider (IaaS, PaaS, etc). Describe and explain the Vendor's approach to preserving and transferring control of the 3rd party cloud infrastructure to the State or its designee during Transition-Out.

c) Transition-Out Period

Using the parameters below, describe Vendor's approach to implement the transition-out phase:

1. Expected Phase Timeframe: No more than four (4) months in duration, unless the Maintenance and Enhancement Phase is extended.
2. The State will initiate the Transition-Out Period during the Maintenance and Enhancement Phase by notifying the Vendor in writing to begin performing Transition-Out Period tasks.
3. The Transition-Out Period will end when the Vendor's Transition-Out Completion Report has been accepted by the State, or when the end date of the Contract has been reached.

3.5.2 OBJECTIVES

- a) Describe how Vendor will provide "Transition-in" services, including
 1. The rehosting (or "lift and shift") of the WIC Crossroads applications and all data (including file system contents) to a Vendor managed cloud infrastructure
 2. Maintaining or substituting any non-State software components required to support WIC Electronic Benefits Transfer (EBT) processing
- b) Describe how Vendor will perform all maintenance to the WIC Crossroads application. Maintenance includes the following items:
 1. Defect correction
 2. Change order implementation
 3. Production help desk support
- c) Describe how Vendor will perform enhancements to the WIC Crossroads application in accordance with the Change Request process Section 3.5 Business and Technical Specifications, Sub-Section 3.5.11 .
- d) Describe how Vendor will provide "Transition-out" services. (A description of a detailed Transition-Out plan is requested in Section 3.5 Business and Technical Specifications, Sub-Section 3.5.14.)
- e) Describe how Vendor proposes to conduct all necessary Crossroads related consultation and training of the WIC EBT Provider and EBT FMNP staff at no additional cost to the State. (A description of Vendor's specific training approach is requested in Section 3.5 Business and Technical Specifications, Sub-Section 3.5.4 and 3.5.5).

Crossroads WIC MIS 30-25002-DCFW

3.5.3 PRODUCT MANAGEMENT

a) Product Staffing

Describe your staffing plan for this contract. (After contract execution, pursuant to the DIT Terms and Conditions, the Vendor will request prior written State approval for changes to personnel who fill the role of any of the Personnel described in this RFP prior to personnel changes occurring. The State also reserves the right to reject any replacement and reserves the right to request a replacement should the State deem it necessary.)

The State envisions a product team that includes the following Personnel, or Vendor's equivalent position/title in 1-4 below:

1. M&E Vendor Product Manager – Describe how this position leads the Vendor's team and is responsible for the overall management of the Contract and the completion of all required tasks and activities during the Contract. Please include the name and describe the relevant experience and qualifications of the proposed person. In lieu of the description, Vendor may provide a Curriculum Vitae (CV) for the resource proposed for this position.
2. M&E Vendor Development Manager – Describe how this position leads the Vendor's technical team during both the Transition-In Phase and M&E Phase (including transition-out) of the Contract and assists the State in ongoing technical management. Please include the name, and describe the relevant experience and qualifications of the proposed person. In lieu of the description, Vendor may provide a Curriculum Vitae (CV) for the resource proposed for this position.

Describe the responsibilities of this position for:

- a. Generating System designs;
 - b. Coordination and execution of the system interface between Crossroads and the EBT system;
 - c. Coordination and execution of the Crossroads system configuration and architecture changes.
3. M&E Vendor Test Manager – Describe how this position leads the Vendor's testing team during the Contract. Please include the name and describe the relevant experience and qualifications of the proposed person. In lieu of the description, Vendor may provide a Curriculum Vitae (CV) for the resource proposed for this position. Describe the responsibilities of this position for:
 - a. Functional, End-to-End, System life cycle, and performance testing oversight during maintenance and enhancement phases;
 - b. UAT testing oversight and support;
 - c. Test script or other artifact development;
 - d. Test reports
 4. M&E Vendor Business Analyst Manager – Describe how this position leads the Vendor's Business Analyst team during the Contract. Please include the name and describe the relevant experience and qualifications of the proposed person. In lieu of the description,

Vendor may provide a Curriculum Vitae (CV) for the resource proposed for this position. Describe the responsibilities of this position for:

- a. Creating Change Requests Responses and Estimates;
 - b. Supporting Help Desk assistance requests, including data correction;
 - c. Ensuring test scripts and other artifacts to satisfy State business needs
5. Describe and diagram the organization of the proposed product team, including identification of the key Personnel noted above by name, position title, and responsibilities, lines of authority among and between the various Personnel and any subcontractors that may be used on this product, and whether any Personnel will be hired upon Contract award. Include available letter(s) of intent to accept employment from any such Personnel that are to be hired after Contract award.
6. Describe how Vendor will ensure that the Personnel resources are readily available to the State and how those resources will be able to fully support the Crossroads product.
7. Describe how the State will be able to contact Vendor Position resources, and the escalation path that would be followed to ensure that the State can establish contact with the personnel who fill the role of any of the Personnel when critical needs arise and during critical product periods between the hours of 7:00 am and 7:00 pm Eastern Time, seven (7) Calendar days a week.
8. Describe the staffing approach to include any subcontractor staff.
9. Describe specific steps the Vendor will take to ensure retention of applicable staff during transition-out, to remain compliant with all Contract requirements and SLA until the Contract expires or is terminated.
10. The following are the current roles and responsibilities for the North Carolina DHHS WIC solution, for the Vendor to consider in its proposed organization. Figure 2 illustrates the Organization Structure:

Figure 2 - North Carolina Crossroads Organizational Structure

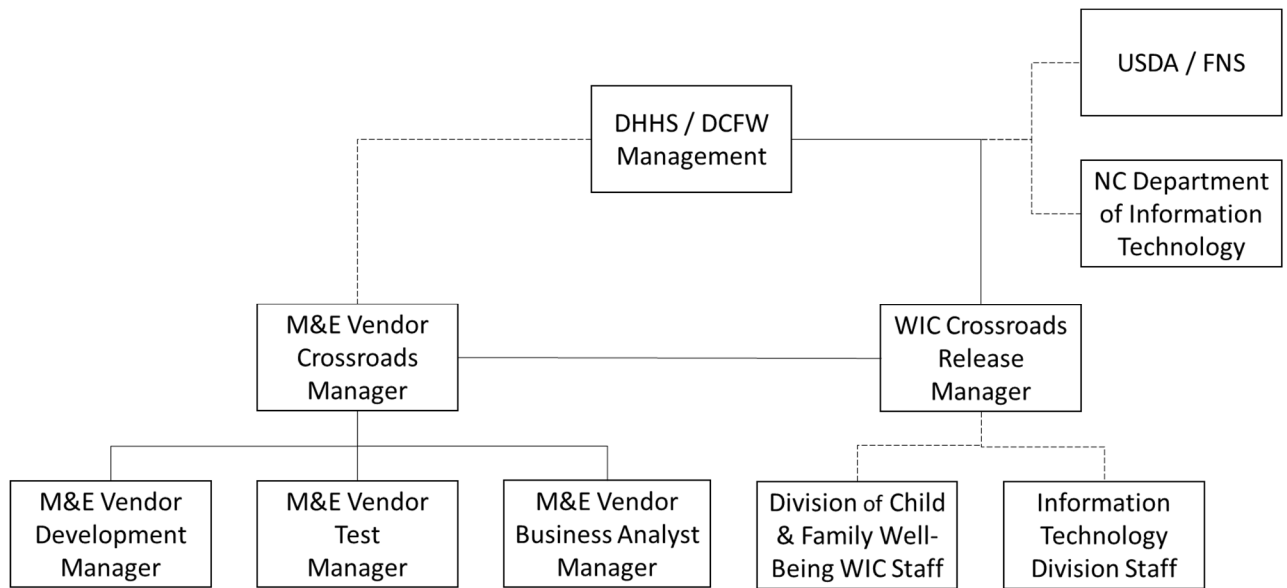


Figure 2: Position Descriptions:

1. DHHS Crossroads Release Manager tasks:

- a. Serve as the Agency Project Manager referenced under Section 7.11 Project Management
- b. Ensure all Contract instruments are appropriately executed.
- c. Provide validation of deliverable acceptance and performance measurements.
- d. Schedule and validate that Contract milestones, timelines, and deliverables are provided pursuant to the Contract performance measurements.
- e. Facilitate Contract review by the DHHS Information Technology Division, Department of Information Technology (DIT), Office of Purchase and Contract Services, and the Attorney General's Office.
- f. Provide Contract and Vendor oversight.
- g. Assure deliverables are of high quality and meet the business requirements.
- h. Monitor the product and Contract to ensure delivery of complete, accepted deliverables on schedule.
- i. Designate signatories for deliverables and recommend approval of payments.
- j. Prioritize, review and approve cost estimates, timelines, formats, outlines and product deliverables.
- k. Ensure proper technical stakeholder involvement.
- l. Initiate and participate in Product Team meetings.
- m. Review and provide input on draft documents.
- n. Determine risk.
- o. Participate in work sessions for the development of specifications

2. DHHS Crossroads DCFW/WIC and ITD Staff tasks:

- a. Participate in work sessions for the development of specifications.
- b. Review and provide input on draft documents.
- c. Collaborate with the Vendor on technical issues, Vendor and UAT test plans, schedules, and specifications.
- d. Perform UAT.
- e. Review deliverables and participate in JAD, code and test walk-through sessions.

3. M&E Vendor Product Manager tasks

- a. Serve as the Vendor's Contract Administrator, and the Vendor Project Manager as referenced under Section 7.11 Project Management
- b. Have full authority to commit the Vendor on matters concerning the Contract, including but not limited to: invoices, negotiating and approving change requests, and taking all actions necessary to ensure Contract compliance and proper performance for all tasks within the milestones.
- c. Deliver Contract performance measurements, reporting and tracking documents and all other documentation as scheduled and/or required by the Contract.
- d. Serve as the primary contact to interface with the DHHS Release Manager, the DHHS Information Technology Division, the DHHS Office of Purchase and Contract Services, Third Party Vendors, and DIT as it pertains to any Contract obligations.
- e. Notify the DHHS Release Manager, verbally within one (1) Business Hour and in writing within one (1) Business Day, when the Vendor discovers any problem(s) that may jeopardize the successful or timely completion of the Vendor's Contract obligations.
- f. Ensure that the Vendor Team fulfills its duties and responsibilities under the Contract.
- g. Escalate issues to the DHHS Release Manager or designee.
- h. Have the responsibility over the Vendor Team to ensure compliance with the Contract and tasks with the approved work plan.
- i. Develop and submit all deliverables as required by this Contract.
- j. Ensure that the Vendor meets the Product Schedule and milestones as defined in the Work Plan and the Contract.
- k. Provide sufficient copies of materials for meetings.
- l. Attend, participate, facilitate, prepare materials for and document executive status briefings and other meetings as needed and requested by DHHS.
- m. Provide support for troubleshooting any known technical problems and issues as reported by the DHHS Crossroads WIC and ITD staff. If a problem is known and reported by DHHS, the Vendor Product Manager will coordinate having the problem fixed/resolved, in accordance with the Risks/Issues Management Plan and the ongoing Contract.
- n. Provide maintenance support as outlined in the Contract.

b) Product Management Plan

Describe Vendor's Product Management Plan (PMP) that outlines the Vendor's proposed product management approach for this product. The Product Management Plan is the overarching "umbrella" Plan that defines how the contract is executed, monitored, controlled, and closed. Vendor may provide the plan description within the body of the text of the Vendor's

proposal, or provide a separate section or attachment. Describe (at a high level) the Vendor's approach to at least the following topics:

Scope Management	Schedule Management	Quality Management	Staffing Management
Database Queries and Scripting	Risk and Issues Management	System Design and Development Management	Capacity Management
Status Reporting	Change Management	Product Governance	Training Management
Test Management	Security and Vulnerability Management	Disaster Recovery	Help Desk Support
Action Item Tracking Tool	Release Management	Documents, Deliverables, and Records Management	Collaboration Web Site
Transition-In Management	NC Technical Architecture System Design (TASD)	Software Build Tools	Transition-Out Management

Describe the following:

1. The points of contact between the Vendor and the State and the level of decision-making authority these positions will have.
2. The proposed levels of staffing, including technical staff, to ensure all deployment, ongoing, and transition-out operational tasks and responsibilities are completed in a timely and accurate manner. At a minimum, Vendor's proposed levels of staffing will be such that the following specifications can be met:
 - a. Notifying designated State staff within one (1) hour in the event a situation occurs that might adversely affect system deployment, ongoing system operations, or 3rd party system such as EBT.
 - b. Providing a Change Request (CR) Response as outlined in the Change Request Process.
 - c. Providing CR Draft Estimates as outlined in the Change Request Process.
 - d. Providing appropriate technical staff so that approved CR Estimates are developed, tested, and delivered for UAT as outlined in Change Request Process.
 - e. Providing appropriate technical staff for the timely and accurate correction of all system defects in accordance with all SLA requirements. A temporary workaround for production down or critical system defects with the core business processes that prevent the certification of WIC participants, the issuance of WIC benefits, reconciliation of redeemed benefits, generation of rebates, and transmission/reception of EBT files will be developed and implemented as stipulated in **Table 3 - Service Level Agreement**.
3. The industry best practice development methodology to be used by the Vendor, adhere to best practices for development coding standards, and include detailed comments

within the source code, using only the English language, explaining system modifications and issues resolved.

4. How Vendor will provide staffing for the Help Desk so that all incoming calls, emails, or issues in the reporting system are answered within the period defined in the SLA.
5. The Vendor's product management approach to ensure that the above SLA requirements are met.
6. Vendor's experiences with meeting time-sensitive special needs of a state agency. For example, describe any experiences with implementing MIS functionality changes as part of a states' response to COVID-19.
7. Other aspects, if any, of Vendor's proposed product management approach.

c) Transition-In Phase Plan

The purpose of the Transition-In Phase is to facilitate the transition of full responsibility for supporting Crossroads from the incumbent vendor to cloud environments managed by the awarded Vendor.

1. Describe Vendor's proposed Transition-In Plan to address how Vendor will perform the tasks needed to successfully transition Maintenance and Enhancement Services from the previous Vendor.
2. Describe in your Transition-In Plan, in detail, Vendor's approach to each of the following Transition-In Phase specifications:
 - a. Coordinate an onsite Kickoff Meeting within four (4) weeks of the Contract effective start date, with appropriate State staff and the incumbent Crossroads vendor, to be held at State facilities in Raleigh, North Carolina.
 - b. Attend any additional training sessions with the incumbent vendor, either virtual or onsite, as requested by the State, at a location within or outside of North Carolina, to be determined by the State.
 - c. Transition-in the Crossroads source code and system documentation from the incumbent vendor, to compile and produce the Vendor's first installable internal system test build of Crossroads within ninety (90) Calendar Days of Contract Execution.
 - d. Request any needed State-owned hardware for consideration by the State for approval.
 - e. Submit applicable Document Deliverables listed in Table 1 – List of Product Deliverables
 - f. Import DFDD and Risk Code documentation, User Manuals, DTS and White Papers, Data Dictionary, ICD, ECD, RDD, Installation and Configuration Instructions, and the CPS Operations Manual.
 - g. Import regression and performance test artifacts.
 - h. Begin Change Request and Release planning and execution for M&E Phase.
 - i. Deploy issue reporting system and secure FTP site.

- j. Deploy action item tracking tool.
- k. Deploy collaboration web site.
- l. Deploy Help Desk contact infrastructure.
- m. Request all needed access and NCID credentials for State environment support.
- n. Obtain and submit signed Non-Disclosure Agreements within fifteen (15) Calendar days of Contract Award for all Vendor staff who will have access to Crossroads Confidential Information.
- o. Deploy the Vendor's internal development and test environments needed to compile and install changes to the source code.
- p. Deploy functioning solutions of the WIC Crossroads solutions (applications and data including file systems) into the Vendor managed cloud environments for State production, State UAT, and State Staging within one hundred twenty (120) Calendar Days of Contract Execution. Any changes to the Crossroads systems needed to successfully integrate them into the cloud platform will be performed at no additional cost.
- q. Provide State personnel (to be determined at the sole discretion of the State) with all necessary access credentials, database permissions, training, and client software requirements needed to execute read-only (R/O) queries and other scripting against all production and non-production Vendor-managed databases
- r. At no additional cost, the Vendor will obtain all necessary third party software/IaaS/PaaS/SaaS licenses for Vendor's Services for the Crossroads solution in the Vendor-managed Production and non-Prod environments, including but not limited to cloud computing platforms, networking services, operating systems, database software, software deployment solutions, and storage.

d) Joint Application Design (JAD) Sessions for Change Requests

Describe the approach and types of JAD sessions the Vendor would facilitate to develop specific requirements to implement Change Requests. The Vendor will have designated staff, that is not facilitating the meeting, present and available to document decisions and action items. All JAD sessions will be conducted either virtual or in Raleigh, North Carolina, to be determined by the State. Onsite sessions in Raleigh may be required only for significant new functionality.

e) Transition-In and Transition-Out Communications

1. Describe the Vendor's process, frequency and format for meetings, conference calls and onsite visits during transition-in and transition-out phases, as well as status reports.
2. Explain how the Vendor will provide a written summary, including but not limited to, the status of the Vendor's activities (completed since last update, new since last update, scheduled since last update, etc.), accomplishments, action items (those to be completed by the Vendor and by the State), and any new or changed risks or issues. Transition-In and Transition-Out communications will include such topics as:

- a. Tasks accomplished this period
- b. Deliverables submitted this period
- c. Outstanding tasks/deliverables
- d. Risk tracking log
- e. Outstanding problems, issues, and changes
- f. Function and architecture training agendas and action item lists for the application, batch, reporting, and portal areas.
- g. Minutes from source code and documentation walkthrough sessions
- h. Minutes from known defect walkthrough sessions
- i. Minutes from tool, hardware, and configuration walkthrough sessions that produce and install executable builds

f) Maintenance and Enhancement Communications

Explain the Vendor's process, frequency, format, and timeline for Maintenance meetings, conference calls and onsite visits during Maintenance, as well as status reports. Explain the process for providing a written summary, including but not limited to, the status of the Vendor's activities (completed since last update, new since last update, scheduled since last update, etc.), accomplishments, action items (those to be completed by the Vendor and by the State), and any new or changed risks or issues. Maintenance status reports will be monthly no-cost deliverables submitted alongside the monthly M&E invoices, will be in addition to transition-in and transition-out communications, and will include such topics as:

- 1. Defects and defect resolution
- 2. Risk tracking log
- 3. Service Level Agreement (SLA) attainment
- 4. Change Request status

g) Product Work Plan

Describe the Vendor's process, frequency, and format for providing and maintaining a Product Work Plan, that includes the following information:

- 1. Detailed product schedule including tasks required for Transition-In, the modification and deployment of Crossroads Change Requests and System Releases, and Transition-Out. Once the product schedule is approved by the State, any changes to dates and milestones will be approved by the State.
- 2. The product scheduling software to be used by the Vendor to generate the product schedule. Any proposed software will produce files in Microsoft Project Plan (MPP) data file format editable by Microsoft Project 365.
- 3. Work Breakdown Structure (WBS) with a graphic depiction that defines the tasks associated with the objectives for the entire scope of the contract. The WBS will be a decomposition of the work to be executed by the entire product team and indicate task dependencies along with start and end dates. The WBS will include all product deliverables, milestones, and activities at a level that allows the State to track progress towards completion.
- 4. Product tasks and deliverables that describe what is required to accomplish the work detailed in the WBS.

5. Note: Vendor may describe the Product Work Plan within the text of Vendor's proposal or provide a separate appendix. A final Product Work Plan will be due after Contract execution for the State's review and approval. The Product Work Plan will be updated with actual completion dates when final deliverables are accepted by the State.

THE REST OF THIS PAGE INTENTIONALLY LEFT BLANK.

6. The following is a tentative schedule of major milestones for an agile/waterfall hybrid approach.

Table 2 - Crossroads Release Schedule

Activity / Milestone Event	Tentative Dates
Contract Execution Start Date	August 1, 2025
Contract Kickoff Complete	August 31, 2025
Contract Transition-In (non-incumbents)	August 1, 2025 - March 31, 2026
Lift and shift Test and Production systems to cloud	August 1, 2025 - March 31, 2026
Release 1.40 Development	April 1, 2026 - May 31, 2026
Release 1.40 UAT and Deployment	June 1, 2026 - September 30, 2026
Release 1.41 Development, UAT, Deployment	June 1, 2026 - January 31, 2027
Release 1.42 Development, UAT, Deployment	October 1, 2026 - May 31, 2027
Release 1.43 Development, UAT, Deployment	February 1, 2027 - September 30, 2027
Release 1.44 Development, UAT, Deployment	June 1, 2027 - January 31, 2028
Release 1.45 Development, UAT, Deployment	October 1, 2027 - May 31, 2028
Release 1.46 Development, UAT, Deployment	February 1, 2028 - September 30, 2028
Release 1.47 Development, UAT, Deployment	June 1, 2028 - January 31, 2029
Release 1.48 Development, UAT, Deployment	October 1, 2028 - May 31, 2029
Release 1.49 Development, UAT, Deployment	February 1, 2029 - September 30, 2029
Release 1.50 Development, UAT, Deployment	June 1, 2029 - January 31, 2030
Release 1.51 Development, UAT, Deployment	October 1, 2029 - May 31, 2030
Release 1.52 Development, UAT, Deployment	February 1, 2030 - September 30, 2030
Release 1.53 Development, UAT, Deployment	June 1, 2030 - January 31, 2031
Release 1.54 Development, UAT, Deployment	October 1, 2030 - May 31, 2031
Release 1.55 Development, UAT, Deployment	February 1, 2031 - September 30, 2031
Release 1.56 Development, UAT, Deployment	June 1, 2031 - January 31, 2032
Release 1.57 Development, UAT, Deployment	October 1, 2031 - May 31, 2032
Transition-Out Period Tasks	April 1, 2032 - July 31, 2032
Contract Closeout Complete	July 31, 2032
Optional Contract Year 8	
Release 1.58 Development, UAT, Deployment	February 1, 2032 - September 30, 2032
Release 1.59 Development, UAT, Deployment	June 1, 2032 - January 31, 2033
Release 1.60 Development, UAT, Deployment	October 1, 2032 - May 31, 2033
Transition-Out Period Tasks	April 1, 2033 - July 31, 2033
Contract Closeout Complete	July 31, 2033
Optional Contract Year 9	
Release 1.61 Development, UAT, Deployment	February 1, 2033 - September 30, 2033
Release 1.62 Development, UAT, Deployment	June 1, 2033 - January 31, 2034
Release 1.63 Development, UAT, Deployment	October 1, 2033 - May 31, 2034
Transition-Out Period Tasks	April 1, 2034 - July 31, 2034
Contract Closeout Complete	July 31, 2034
Optional Contract Year 10	
Release 1.64 Development, UAT, Deployment	February 1, 2034 - September 30, 2034
Release 1.65 Development, UAT, Deployment	June 1, 2034 - January 31, 2035
Release 1.66 Development, UAT, Deployment	October 1, 2034 - May 31, 2035
Transition-Out Period Tasks	April 1, 2035 - July 31, 2035
Contract Closeout Complete	July 31, 2035

The above release nomenclature and release schedule is tentative and subject to change.

h) Communication and Coordination Plan

1. Describe Vendor's Communication and Coordination Plan including the following information.
 - a. Vendor's communication approach, including events such as status reports, conference calls with various levels of State staff, webinars, onsite visits, etc.
 - b. All stakeholders involved with the product, including the State, the WIC EBT Provider, the Vendor and its subcontractors, and other major related parties.
 - c. How communications among and between stakeholders will be delivered and managed. This will include coordination among the units of the Vendor's product team, including product management, development, testing, and help desk.
2. Describe an overview of the communications approach that will be used with this product. The Communication and Coordination Plan description should include the following tasks:
 - a. Vendor will attend an annual onsite meeting to be held in Raleigh, NC.
 - b. Describe the Vendor's approach to hosting a weekly conference call or webinar as needed by the State of the Release Manager and State Subject Matter Experts to discuss topics requested by both the State and the Vendor.
 - c. Describe an action item tracking tool, compatible with Microsoft Edge , to be hosted by the Vendor and utilized by State staff.
 - d. Describe the Vendor's approach to hosting a collaboration web site, compatible with Microsoft Edge, to facilitate the sharing of documentation and other communication with various State staff.
 - e. Describe the software available to the Vendor to host webinars or other web conferencing. Vendor webinar software will not impose any licensing or location restrictions on the State.
 - f. Describe how communication will be coordinated with the WIC EBT Provider, and EBT FMNP Provider, for any activities related to these EBT interfaces.

i) Quality Assurance Plan

Describe Vendor's Quality Assurance (QA) Management Plan that includes the following information:

1. Describe the Vendor's quality assurance procedures as to how the Vendor will ensure that the Crossroads Product deliverables are of acceptable quality before they are delivered to the State. This includes describing the ability to advance the system clock of test environments as needed for life cycle testing.
2. Describe the Vendor's approach to the various testing levels (i.e. development, Integration, and User Acceptance), in both for maintenance and enhancements, to ensure that the Crossroads system meets the State's expectations and requirements.
3. Describe how quality of the QA Plan is measured, when quality checks occur and how corrective actions are determined and implemented.
4. Both the State and USDA/FNS reserve the option to have a Quality Assurance (QA) Vendor or an Independent Verification and Validation (IV&V) Vendor provide third-party services for the Crossroads Product. Describe in the QA Plan the process for the Vendor to work with the third-party vendor, including hosting onsite visits to the Vendor's facilities, on recommendations and findings provided by the third-party.

5. Describe the Vendor's approach in maintaining a repository of Regression Test artifacts, for use by the Vendor during the various testing levels and to meet the SLA under **Table 3 - Service Level Agreement**. This repository will be exported to the State upon request.

j) Risk and Issues Management Plan

Describe a Risk and Issues Management Plan that includes the following:

1. Describe the Vendor's procedures for how the Vendor will identify, report, monitor, and recommend mitigation strategies for Risks and Issues.
2. Identify who on the Vendor's Product Team is responsible for these activities.
3. Describe a Risks and Issues Management Plan (that consists of a high-level overview of the Vendor's Risk Management processes).
4. Describe the Vendor's approach in providing a Risk Matrix and Issues Log as product control deliverables throughout the term of the contract.
5. Describe the Vendor's approach to perform a risk assessment and security assessment as defined by DHHS Privacy & Security Policy either through third-party or self-assessment on a three-year cycle (with a third-party assessment mandated every third year at the sole discretion of the State).
6. Describe the Vendor's approach to document in the above assessments any Vendor (including subcontractors) intention to utilize offshore resources as stipulated in Attachment F.

k) Configuration Management / Release Management Plan

Describe a Configuration Management / Release Management Plan that includes the following information:

1. Describe Vendor's procedures for how the Vendor manages configurable items and maintains version control over deliverables, source code, installation tools, test scripts, etc.
2. Describe the Vendor's Release Management processes, describing the Vendor's library system for managing North Carolina specific code and releases for defect remediation, including hotfixes.
3. Describe how the Vendor will coordinate releases with the WIC EBT Provider.
4. Describe the Vendor's process to adhere to the incumbent Release "x.x.x.x" nomenclature unless otherwise directed by the State.
5. Describe how the Vendor will support up to three (3) different major releases of Crossroads installed in separate state environments, for example 1.42 in production, 1.43 in UAT, and 1.41 in a secondary test environment.

l) Service Level Agreement

1. Describe Vendor's approach to comply with the following Service Level Agreement (SLA) provisions shown in **Table 3 - Service Level Agreement**, indicating agreement to the liquidated damages for each specific item for which a Service Level is established.
2. Define the process for monthly invoice reductions for not maintaining the minimum threshold of acceptable service level, with carry over to subsequent months should cumulative liquidated damages exceed a single monthly invoice, or problems with service extend beyond a single month.

3. The Vendor's approach should include a description of the format and frequency for reporting compliance.

Table 3 - Service Level Agreement

Liquidated Damages. The State and the Vendor agree to the specific standards set forth in this Contract. Vendor shall maintain and follow the Service Level Agreement below. It is agreed between the Vendor and the State that the failure to meet the Service/Performance Levels identified in the Service Level Agreement below would cause damages to the State that would be difficult or impossible to determine with accuracy. The Vendor agrees that its failure to meet the Service/Performance Level may or will affect the delivery of (goods/services, etc.), either directly or indirectly and may or will result, directly or proximately, in monetary damages to the State; therefore, the actual amount of such injury and damage will be impossible or extremely difficult to calculate. The State and the Vendor therefore agree that the liquidated damages set out in the table below shall be a reasonable approximation of the damages that shall be suffered by the State.

- 1) Vendor agrees that the Vendor shall pay liquidated damages to the State in the instances and in the amounts set forth in the below table. The Parties also agree that the stated liquidated damage amounts are reasonable and not punitive. Accordingly, in the event of such damages, at the written direction of the State, the Vendor shall pay the State the indicated amount as liquidated damages, and not as a penalty.
- 2) Amounts due the State as liquidated damages, if not paid by the Vendor within fifteen (15) days of notification of assessment, may be deducted by the State from any money payable to the Vendor pursuant to this Contract. The State will notify the Vendor in writing of any claim for liquidated damages pursuant to this paragraph on or before the date the State deducts such sums from money payable to the Vendor. No delay by the State in assessing or collecting liquidated damages shall be construed as a waiver of such rights. The imposition and payment of liquidated damages shall not affect or waive any other rights of the State to enforce or terminate this Contract. In cases where actual damages can be determined, liquidated damages shall not apply.
- 3) If the State elects not to impose liquidated damages in a particular instance, this decision shall not be construed as a waiver of the State's right to pursue future assessment of performance standards and associated liquidated damages; nor construed to limit any additional remedies available to the State.
- 4) The Vendor shall not be liable for liquidated damages when, in the opinion of the State, incidents or delays result directly from causes beyond the control and without the fault or negligence of the Vendor. Such causes may include, but are not restricted to, acts of God, fires, floods, epidemics, labor unrest, and third-party carrier matters outside the control of Vendor; but in every case the delays must be beyond the control and without the fault or negligence of the Vendor.

The Service performance Levels and liquidated damage for each are as follows:

Criteria	Liquidated Damages	
(1) Statewide production down or other critical statewide issue due to software Defect, or incorrect installation/configuration by Vendor, not circumvented (defined as the core business processes under the PMP) by Vendor in six (6) Business Hours from initial report and continuing every following Business Day.	Liquidated Damage rate starting at six (6) Business Hours, plus additional penalty rate for each Business Day.	

(2) Any production Defect, that the State specifies severely affects statewide operations or reporting, that is not corrected in production by Vendor within two (2) calendar weeks of initial report.	Liquidated Damage rate times whole number of delayed Calendar Weeks from the initial report.	Liquidated Damage Rate is 25% x Monthly Maintenance and Enhancement Phase Cost (Table 3)
(3) Each Defect due to inaccurate or unavailable participation counting, that escaped Vendor regression testing and is discovered in production. This is in addition to Criteria (2).	Liquidated Damage rate times fixed factor of one-half (1/2), per each Defect.	
(4) One or more Defects created or reopened by the State during UAT, unresolved and causing two or more calendar week production Deploy delay of a major release. Liquidated Damage accrual stops if Deployment cancelled at sole discretion of the State.	1/2 of the Liquidated Damage rate times the whole number of delayed Calendar Weeks from the stipulated Deployment date.	
(5) Two or more Calendar Week delay in release delivery for any agreed UAT start.	1/2 of the Liquidated Damage rate times the whole number of delayed Calendar Weeks from initial due date.	
(6) For each CR, initial or revised CR pricing or draft content not delivered within two Calendar Weeks after each stipulated date, continuing every two Calendar Weeks.	1/8 of the Liquidated Damage rate starting at two (2) Calendar Weeks, plus 1/8 of the liquidated damage rate for each additional two (2) Calendar Week delay until CR delivery is completed. This is cumulative across all CRs requested.	
(7) Less than 80% of stipulated Defect fix count or CR hours delivered in each UAT release cycle.	Liquidated Damage rate times fixed factor of two (2).	
(8) Four calendar week delay in delivery of revised system documentation as stipulated, continuing every two Calendar Weeks.	Liquidated Damage rate starting at four Calendar Weeks, plus a penalty rate for each additional two Calendar Week delay until documentation delivery is completed.	

The illustration below shows fictitious examples of how monthly payments may be reduced to the Crossroads Vendor due to failure to meet SLA criteria, based on an imaginary M&E Cost:

Monthly M&E Invoices before Liquidated Damages		Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan
Liquidated Damage Rate is 25% of Monthly Phase Cost		\$32,000	\$32,000	\$32,000	\$32,000	\$32,000	\$32,000	\$32,000	\$32,000	\$32,000	\$32,000	\$32,000	\$32,000
		\$8,000	\$8,000	\$8,000	\$8,000	\$8,000	\$8,000	\$8,000	\$8,000	\$8,000	\$8,000	\$8,000	\$8,000
Liquidated Damage Criteria	Example of Damage Trigger	Liquidated Damages Cost											
(6) For each CR, initial or revised CR pricing or draft content not delivered within two Calendar Weeks after each stipulated date, continuing every two Calendar Weeks.	Two of five requested CR draft revisions were delivered 42 calendar days after stipulated March date.			(\$4,000)	(\$2,000)								
(7) Less than 80% of stipulated Defect fix count or CR hours delivered in each UAT major release cycle.	Agreed defect fixes delivered, but only 150 hours of agreed 200 CR hours delivered for June UAT.					(\$16,000)							
(5) Two or more Calendar Week delay in release delivery for any agreed UAT start.	20 calendar day delay in June UAT delivery.					(\$8,000)							
(2) Any production Defect, that the State specifies severely affects statewide operations or reporting, that is not corrected in production by Vendor within two (2) calendar weeks of initial report.	Inaccurate Formula Rebate Invoice corrected 14 calendar days after issue reported					(\$16,000)							
(1) Statewide production down or other critical statewide issue due to software Defect, or incorrect installation/configuration by Vendor, not circumvented (defined as the core business processes under the PMP) by Vendor in six (6) Business Hours from initial report and continuing every following Business Day.	Production was down due to Vendor defect reported at 10AM Eastern the Wednesday before Thanksgiving holiday, production restored the following Tuesday at 5PM Eastern										(\$16,000)		
Monthly Invoices after Liquidated Damages		\$32,000	\$32,000	\$28,000	\$30,000	\$0	\$24,000	\$32,000	\$32,000	\$32,000	\$16,000	\$32,000	\$32,000

m) Partnerships and Contractual Relationships

Describe Vendor's partnerships and contractual relationships when Vendor uses subcontractor(s) to fulfill the requirements of this RFP. Describe the types of service(s), contractual relationship and the term of the contract between Vendor and its subcontractor(s).

3.5.4 COORDINATION WITH WIC EBT PROVIDER / INTERFACE WITH THE EBT SYSTEM

The State has awarded a separate Contract for WIC EBT in North Carolina whom the State refers to as the "WIC EBT Provider". The Vendor and the WIC EBT Provider will fully cooperate and coordinate activities throughout the life of the current or future WIC EBT contract, including participating in any Transition-Out or Transition-In activities related to any change in WIC EBT contract, at no additional cost to ensure smooth operations and maintenance between the Crossroads and EBT systems.

a) Coordinate Interface with EBT

Describe and explain the Vendor's process to coordinate with the current or any future WIC EBT Provider at no additional cost to the State to ensure that the two systems interface correctly (including providing diagnostic data to assist the WIC EBT Provider in resolving interface problems introduced by either party), and to make such Crossroads modifications as may be necessary to maintain a seamless interface on an ongoing basis for any future WIC EBT modifications that may be required. Describe how the Vendor will maintain an Interface Control Document (ICD) to document and provide the specifications for the interface points between the WIC EBT and Crossroads system.

b) Coordinate Schedules and Testing with EBT

Describe and explain the Vendor's process to coordinate schedules and timelines to ensure that both systems maintain a seamless interface and the process to resolve any scheduling conflicts that might arise. Describe how this process will include internal testing between the Crossroads and WIC EBT systems prior to a Crossroads UAT to certify readiness for UAT.

c) Coordinate Training with EBT

Describe and explain the Vendor's process to coordinate training activities for UAT and deployment, as requested by the State due to a future modification of the interface.

The Vendor will be required to conduct all necessary Crossroads related consultation and training of the WIC EBT Provider staff at no additional cost to the State, in accordance with Section 3.4.2 e). Describe how Vendor will accomplish the foregoing.

3.5.5 COORDINATION WITH EBT FMNP PROVIDER

NC has moved FMNP to an EBT solution. Describe the Vendor's understanding and agreement that the awarded Vendor and the EBT FMNP Provider will fully cooperate and coordinate activities and training throughout the term of any EBT FMNP contract.

3.5.6 PRODUCTION AND NON-PRODUCTION DATA CENTERS

a) Future Expansion

1. The North Carolina WIC Program has the potential to increase caseload quantities. Describe the Vendor's ability and methods to monitor State and Vendor system operations to make specific recommendations if additional processing resources and capacity is required to maintain acceptable processing requirements and timeframes.

2. Describe the approach the Vendor will take to procure additional Vendor system resources or capacity, and the time required to do so, should the need be identified.

b) System Performance

1. Performance testing activities will be described in the QA Plan. Describe the Vendor's approach to performance testing the system after modifications for maintenance and enhancements in their internal test environments.
2. Describe Vendor's approach to monitoring system operations daily, and making necessary mutually agreeable adjustments to maintain peak operation efficiency so that system users are not adversely affected. Describe the type of automated and manual systems that will be used by the Vendor if requested.
3. Describe Vendor's approach to performing mutually agreeable timely database tuning to keep the databases running as efficiently and effectively as possible. Describe the type of automated and manual systems that will be used.
4. Describe Vendor's approach to adhering to the following expected page load and/or response times:
 - a. An average response time of 1-3 seconds for basic transactions such as insert, update, delete, and queries from a single table.
 - b. 5-25 seconds for "complex transactions" – Complex transactions are defined as those that require:
 - i. Data requests from the application database or data store;
 - ii. Dependencies on application work flows or back end processing;
 - iii. Interfaces with external applications or web site.
 - c. 5-200 seconds for generation of ad-hoc reports, depending on complexity and size of each individual report. These reports are generally created using predefined data queries which are optimized for performance. These reports are also generally collecting smaller sub sets of data versus more complex analytical reports.
 - d. 5-30 minutes for generation of complex analytical reports. These types of reports generally require back end processing or complex data queries. Analytical reports are generally built in real time based on queries created by the end user, where the queries are not optimized for performance. These reports also tend to require larger sub sets of data than ad-hoc reports.
5. Describe Vendor's approach to execute Performance testing activities annually (by a mutually agreed upon date) in the Vendor's technical environment, testing Crossroads under full-load and no-load conditions during normal and peak performance periods.
 - a. Describe Vendor's proposal for providing an annual draft Performance Test Plan to the State for approval prior to start of each annual performance test that addresses the criteria listed above.
 - b. Describe the Vendor's approach to evaluating the need for performance testing Crossroads in its internal test environments after the completion of maintenance and Change Request modifications.
 - c. Describe how Vendor will advise State staff on Vendor Performance Test Scripts to perform automated tests on Crossroads as specified by a Test Case.

- d. Describe a Performance Test Results Report that outlines an executive summary and the detailed documented output of the execution of every Test Case for performance testing, which the State will review and approve. For every Test Case, actual test results will be documented, including any necessary re-testing required by the State prior to the delivery of the applicable release for UAT.

c) System Security at Vendor Facilities

The Vendor will be responsible for providing a comprehensive security and vulnerability program that meets applicable State and Federal requirements to protect the integrity and confidentiality of program data. This program will include administrative, physical, technical, and system controls.

1. Describe Vendor's Security and Vulnerability Plan for the following:

- a. The location and description of the controls at each of the physical Vendor facilities where contract-related activities occur to protect data from unauthorized use and access, such as entrance security, use of access cards, restricted access areas, Closed Circuit Television (CCTV), fire protection, etc.
- b. The types of controls, for both Vendor local and cloud based solutions, over the development and testing environment hardware and software to protect data from unauthorized use and access, such as communication access controls, user identification and authentication, system access and audit controls, transaction communication controls, discretionary access controls, separation of duties, data destruction procedures, etc.
- c. The virus and malware controls to protect data from unauthorized use, access, contamination or corruption.
- d. Vendor's plan for the event of a suspected or confirmed Breach, Cybersecurity Incident, or Significant Cybersecurity Incident involving Crossroads or the State's Confidential Information, at the Vendor's own expense:
 - i. immediately report such Breach or incident to the DHHS Privacy and Security Office at <http://www.ncdhhs.gov/about/administrative-divisions-offices/office-privacy-security> (or, if website is unavailable, fax to 919-733-1524) within twenty-four (24) hours after first discovery, as well as to the Contract Administrator and DHHS Release Manager;
 - ii. investigate such suspected or confirmed Breach or incident;
 - iii. provide a remediation plan, acceptable to the State, to address the Breach/incident to prevent any further Breaches/incidents;
 - iv. conduct a forensic investigation to determine what systems, data and information have been affected by such event;
 - v. cooperate with the State, and any law enforcement or regulatory officials, credit reporting companies, and credit card associations investigating such Breach/incident.
- e. The Vendor will update the plan throughout the life of the Contract as industry standards change, new State and/or Federal requirements are issued, or new security or vulnerability concerns are discovered .

2. Describe the process that will be used by the Vendor to notify individual(s) or parties affected by a security incident(s). If any applicable federal, state, or local law, regulation, or rule requires the State's or the Vendor to give affected persons written notice of a Breach arising out of the Vendor's performance under this Contract, the Vendor will bear the cost of the notice ("Notification Related Costs"). Providing notice to affected parties will include the following:
 - a. The date of the notice.
 - b. The reporting entity's name and contact information so that affected individuals can obtain additional assistance or information.
 - c. A brief description of the data breach incident in general terms.
 - d. The date of the breach, if unknown, the approximate date or date range of the breach.
 - e. The categories of personal information at issue.
 - f. A brief description of the actions taken by the Vendor to contain the breach and protect data from further unauthorized access or use.
 - g. Advice on actions affected individuals should take.
 - h. Contact information for national consumer reporting agencies.
 - i. Recommendations for affected individuals to protect themselves. For example, reviewing account statements, monitoring free credit reports, or subscribing to credit reporting services as stipulated in Attachment B.
3. Describe an overview of the security protocol that will be used with this product, including a statement that the protocol complies with all standards and specifications as listed in this RFP. Describe any security issues that may have occurred at the facility that will be used for North Carolina development and testing processing in the past three (3) years and how they were mitigated.
4. Describe approach for Vendor to continue to comply with data retention and notification about a breach of data until the data retention period has expired and the data has been destroyed or purged and the Vendor has provided written certification of such destruction or purge to the State.
5. Describe the Vendor's process for conducting vulnerability scanning and testing against the Crossroads system installed in internal Vendor environments and Vendor-managed State production and test environments, including all web portals, with a minimum of publishing vulnerability results to the State as part of the Security Assessments stipulated in Table 1 – List of Product Deliverables.
6. The State and Vendor may perform vulnerability scans against all Vendor-managed cloud servers. Describe how any vulnerabilities identified by the State or by the Vendor, that are specific to the design of Crossroads, will be corrected by the Vendor in a timely manner at no additional cost to the State.
7. During the execution of the resulting Contract, the Vendor will notify the Contract Administrator and DHHS Crossroads Release Manager within twenty-four (24) hours of any contact by the federal Office for Civil Rights (OCR) received by the Vendor.
8. Describe process and timelines for the Vendor to comply with any State requests for information related to a breach, including but not limited to: root cause analysis, impact, mitigation strategy, technology involved, and timing.

d) Disaster Recovery at Vendor Facilities

The Vendor will be responsible for providing disaster recovery services and staff facilities with this product that minimizes production system downtime to no more than one (1) continuous hour of total service disruption in the event of a disaster. Describe Vendor's Disaster Recovery and Contingency Plan. The Vendor will update the Plan throughout the life of the Contract as necessary. Describe Vendor's Disaster Recovery and Contingency Plan for the following:

1. A description of an evaluation of the types of disasters that may affect the ability of the Crossroads development, testing, or Help Desk staff facilities to operate;
2. A description of the plan to mitigate the effect of such disasters;
3. A description of the disaster recovery facilities that will be used in the event of a disaster;
4. A description of the criteria for determining when the Plan will be invoked, the staff that will be involved, and the timelines for providing notification to the State;
5. A description of how the environments will be restored once the disaster situation has been resolved;
6. A description of how and when the Disaster Recovery Plan will be tested.
7. A description of an overview of the disaster recovery facilities and procedures that will be used with this product.

e) System Requirements for User Hardware and Software

Describe how the Vendor will maintain descriptions in the existing System Documentation of the minimum hardware configurations, including operating systems and web browsers, required to access / operate the System from the computers being used at the State Office level and the clinic level, so that the State can verify that existing hardware / software used by staff is sufficient or whether an update is needed prior to release deployment.

3.5.7 HELP DESK SERVICES

a) General Help Desk Specifications

Describe the Vendor's process for providing system support services to State WIC Office staff (via an unlimited toll-free telephone number, email, and issue reporting system). Customer service will be provided by a facility with staff physically located in the continental United States, as specified in Attachment K. Federal and Other State Specifications .

Describe Vendor's Help Desk Plan that details how the Vendor will provide customer support services and describe the the below elements.

1. Describe the Vendor virtual capabilities that will allow State staff to share workstation images real-time with Help Desk staff.
2. Describe how the Vendor will log and will develop a library of common debugging steps to assist with the resolution of issues (including hardware issues) or the documentation of more complicated issues that get referred to development staff for further research.
3. Describe the Vendor's escalation protocol for handling all calls to ensure that critical calls are handled in a timely and appropriate manner. Include in the explanation a process and a timeline for notifying the State when the determination is made that an issue (critical or non-critical) appears to be system-wide that affects multiple users.

4. Describe the process and frequency of training provided as new help desk staff are hired and/or as additional modification are made to the System prior to the release deployment of such modifications so that staff are fully knowledgeable of the changes.
5. Describe the process of how the Help Desk staff will have access to management and/or technical resources so that issues can be handled in a timely and appropriate manner.
6. Describe the process of how the Help Desk staff will request and maintain access to the production and test/training environments so that the Vendor can research server and application issues on a real-time basis.
7. Describe the process for tracking calls and Help Desk activities that enable the Vendor to monitor and track the volume of calls so that staffing levels may be adjusted accordingly as call volumes dictate.
8. Describe the process to capture and determine common issues that might indicate a system-wide defect, an area where a System modification may be needed to enhance System use, or the need for additional user training.
9. Describe the types of reports that are available that summarize various Help Desk activities and statistics for internal use and for State use. Include sample reports with the response.
10. Describe and explain how the following performance standards for call handling will be met:
 - a. Calls will be answered by live staff within one (1) minute.
 - b. For a critical statewide production down issue reported by any State staff, the Vendor will provide written acknowledgement to the reporting State staff, the Contract Administrator, and the DHHS Release Manager within fifteen (15) minutes that appropriate Vendor staff are working the issue.

b) Help Desk Support for State Users

The Vendor will provide the State WIC Office with technical assistance for Crossroads related issues during normal clinic business hours.

Describe how the Vendor will provide the following services and tasks under this category in 1 through 4 below. For each item, explain how each service and task will be fulfilled.

1. This assistance will be with live staff via telephone, email, and issue reporting system.
2. Normal business hours are defined under Attachment B. Federal or Vendor holidays not observed by the State are considered normal business hours. The State observed holiday schedule is available at the NC Office of State Human Resources website.
3. Providing email support to use for non-essential issues. All emails will be responded to within one (1) Business Day of receipt. If the issue cannot be resolved within that time frame, a reply email is still required within that time frame to acknowledge receipt and to provide a timeline for resolution.
4. Providing an adequate number of qualified staff thoroughly trained in customer service, general technical skills, and specific knowledge about the Crossroads System to handle a minimum of twenty-five (25) issues per quarter.

3.5.8 ISSUE IDENTIFICATION AND CORRECTION FROM USER ACCEPTANCE TESTING OR PRODUCTION

The Vendor will be responsible for providing the following services and tasks under this category after contract execution. Describe Vendor's proposal for providing a draft UAT Readiness Report prior to the start of each UAT release and describe how Vendor will address the elements below.

a) Comprehensive Testing

The UAT Readiness Report will describe how the Vendor provided and supported end-to-end testing of the Crossroads System functionality with comprehensive financial testing until the State was satisfied the System is working properly in accordance with requirements. Testing will involve issuing benefits, redeeming benefits, running reports (such as participation, FNS-798, Not-To-Exceed (NTE), and rebate invoicing), and any other functions requested by the State.

While EBCI is a separate state agency, Crossroads supports EBCI as a local agency within NC. The ability to separate out EBCI redemptions will be maintained in the QA Management Plan and demonstrated in testing for the UAT Readiness Report until the State is satisfied the System is working properly in accordance with requirements. Testing will involve issuing benefits, redeeming benefits, running reports (such as the rebate report), and any other functions requested by the State.

The draft UAT Readiness Report generated after contract execution will include these elements from the QA Management Plan:

1. The types of testing to be performed;
2. The organization of the test team and associated responsibilities;
3. Test database generation;
4. Test case development;
5. Test schedule;
6. Documentation of test results

Describe Vendor's process for creating a Test Plan for use in satisfying UAT Readiness.

b) Testing Process

Describe Vendor's process of providing the results of the Vendor's internal testing (unit, integration, performance, end-to-end, life cycle, regression testing, connectivity testing, etc.) A walkthrough of the System to demonstrate that the System is functional and ready for each release UAT will be provided to the State if requested.

1. Describe how the Test process will contribute to the thorough quality assurance testing of all software releases, reference database table updates, defect fixes and other Change Requests, are implemented without issue, in accordance with the SLA.
2. Describe how Vendor will provide a written report of release testing results, which the State will review and approve before a release is delivered for UAT.
3. Describe Vendor's process for additional testing that may be required by the State prior to delivery of a release for UAT.

c) Testing Environment

Describe how the Vendor test environment will be seeded with applicable hardware and data like what will be used for UAT, with all necessary tables populated, etc., so that the System may be fully tested prior to release deployment and as any change requests are developed.

d) Coordinate with Outside Entities

Describe and explain how the Vendor will coordinate with outside entities (for example, WIC EBT Provider, other third-party interfaces) to ensure that all interfaces and connectivity can be tested.

e) Test Cases / Test Scenarios / Test Scripts and Results

The Vendor will provide test cases / test scenarios / test scripts after contract execution to be used by UAT staff, if requested by the State. Describe in Vendor's proposal the tool and format which Vendor proposes to use to deliver these test artifacts to the State. The test case scenarios will include scenarios that test the System overall, including end of day, end of month, reporting, and disaster recovery activities. The Vendor will work with the State to identify those common scenarios. Test scenarios that need to be re-run due to defects/testing errors will have an identifier in the Test Case Number.

1. The test cases will include the following:

- a. Test Case Number;
- b. Date created;
- c. Author;
- d. Description of Case;
- e. Type of Test;
- f. Required Inputs;
- g. Steps;
- h. Required Set-Up (Preconditions);
- i. Expected Results;

2. Provide Test Results

- a. Actual results;
- b. Run date;
- c. Tester;
- d. Pass / Pass with Exception / Fail;
- e. Failure or Exception reason;
- f. Defects Identified

f) Virtual Training for the UAT Testing Staff

Describe instructor-led virtual training for the UAT testing staff for topics, if requested by the State and at no additional cost to the State.

g) Describe Onsite Testing Support

Describe a plan for onsite staff to support UAT, if requested by the State.

h) Issue Reporting from Test or Production

Describe the issue reporting system that the Vendor will provide for UAT testers and State Production users to log issues. The Vendor may also propose to use this issue reporting system as the action item tracking tool. The State currently uses Azure DevOps hosted by the incumbent vendor.

1. Describe how the issue reporting system will be hosted by the Vendor, will be browser based and compatible with Microsoft Edge, and not require the licensing or installation of any third-party software on State workstations.
2. Describe how the issue reporting system has the capability to allow users to upload file attachments.
3. Describe the Vendor process to meet WIC confidentiality requirements (7 CFR Part 246.26), such as providing a secure FTP site where sensitive data that cannot be redacted in the issue reporting system can be uploaded by the State to the secure FTP site.
4. Describe how the issue reporting system will have a mechanism for all users to label or tag individual issues in the reporting system with custom labels or tags designed by each user, allowing custom report queries to be executed against the issue database by any user.
5. Describe how the issue reporting system will preserve the date an issue is created, and the date an issue is closed.
6. Describe how the issue reporting system can provide an indicator to distinguish between questions or issues identified by the State in test, identified by the State in production, and identified by the Vendor during their internal efforts.
7. Describe how the Vendor's issue reporting system can be used by the State to log defects that require correction or explanation, requests for additional education and training in functional areas that are working as designed (including any third-party interfaces such as the EBT Provider), and requests for data correction.
8. Describe how the issue reporting system will provide a mechanism for users to create custom queries to identify which issues are in process with the Vendor, and which issues have been returned to the State for retest and closure.
9. Describe how the issue reporting system will have a mechanism for users to subscribe to issue(s) in the reporting system, receiving an email notification of updates to the issues(s).
10. Describe how the Vendor will not close any issues in the issue reporting system without the written permission of the DHHS Release Manager.
11. Describe how, or if, the State may elect to not close an issue until the correction has been monitored by the State and accepted in the production environment.
12. Describe how the Vendor will have a mechanism for mass export of all reported issues and file attachments contained in the issue reporting system, with Vendor performing such mass export upon request of the State.

13. Describe the Vendor's process for granting access credentials to the issue reporting system to third parties upon the request of the State.
14. Describe the Vendor's process for partitioning the issue track system, such that access credentials for each stakeholder can be granted or revoked for each partition.

i) Describe the Defect / Issue Fix Process

Describe and explain the process and timeline to fix defects or issues, identified in test or production, in a timely fashion to allow retesting to verify that the identified defects or issues have been corrected. Defects found will be classified by the State using a scale of one (1) to five (5) using a system with similar criteria.

Table 4 - Defect / Issue Classification Criteria

Priority Level	Criteria
1	Critical Component Failure: Does not allow testing to continue Major malfunction in the System
2	Major Component Failure: Does not allow testing to continue Defect or malfunction in certain areas of the System Problem must be resolved
3	Medium Functional Problem: Testing can continue Functions in certain components do not work properly Components can still work with other components of the System
4	Minor Issue: Testing can continue Minor editing error found in a System component
5	Trivial Issue: Testing can continue Design Clarification issue Future enhancement to the System Cosmetic change needed

Vendors may propose an alternative Priority / Criteria scheme, that aligns with the issue reporting system.

j) Time and Cost to Correct Defects

Describe how all defects will be corrected within the time provided in the SLA, at no additional cost to the State. All identified defects will be corrected before the System can be certified as ready for release deployment. Exceptions may be granted by the State if the State determines that there are sufficient alternative processes in place to mitigate the effects of the defect.

1. For reported defects that require software code fixes, describe Vendor's the development and test capacity to correct a minimum of thirty (30) defects per quarter, aggregated from defects reported in both UAT and production.
2. Historically, North Carolina reports approximately sixty (60) non-production and production issues per quarter. These issues include defects that require software code

fixes, require non-code fixes to system configuration or system data, or require additional training of State staff.

k) UAT Completion Report

Describe the Vendor's comprehensive checklist of items that will be included in each UAT Completion Report, to demonstrate the successful completion of each release UAT and the readiness of the System to move to deployment. The Vendor will provide a formal presentation to the State if requested, including a written certification report that the System is ready to proceed to deployment.

l) IV&V / QA

The State or FNS may utilize outside Vendors to perform third-party Quality Assurance or Independent Verification and Validation activities throughout the course of this contract. The Crossroads Vendor will be responsible for coordinating / cooperating with these QA / IV&V Vendors.

Describe Vendor's experiences in working with IV&V / QA Contractors on WIC MIS, WIC EBT, or other similar projects.

m) Data Correction

Describe the Vendor's approach to perform test or production data correction, upon request of the State and with written permission from the State, as needed for data issues where it is not possible or practical for the State to correct, such as correcting corrupted/non-editable fields, correcting inaccurate data caused by software problems, etc.

1. Describe how this data correction, for issues both due to actions of the State and actions of the Vendor, can be performed by the Vendor at no additional cost to the State.
2. Describe how results of testing of the data correction will be provided to the State upon request and accepted by the State prior to execution of the data correction in a production environment.

3.5.9 INSTALLATION SUPPORT FOR NEW BUILDS OF THE CROSSROADS SYSTEM

Describe Vendor's approach to provide installation support, as listed below, for the Crossroads system for a maximum of six (6) Vendor-managed cloud environments, such as UAT, various secondary testing, production, etc. These environments will be determined by the State and be itemized in a matrix to be maintained by the Vendor.

- a) Describe how the Vendor will coordinate scheduling and installation procedures with technical staff in North Carolina and how the Vendor will request and maintain access credentials to applicable servers that have been granted to the Vendor.
- b) Describe how the Vendor will upload the Crossroads system to the appropriate cloud server(s) to support a statewide deployment and will perform necessary backups of the application and databases as a contingency.
- c) Describe how the Vendor will unpack and install the products into the rehosted servers (web application server, database server, report server, and batch server) as required for the cloud deployment, including how Vendor will execute all necessary database scripts. And how Vendor will not embed or execute any script against an environment's database without prior written approval from the State.

- d) Describe how the Vendor will stop and start Crossroads services as required during the deployment, including the Vendor coordinating with State staff depending on access privileges granted to the Vendor.
- e) Describe how the Vendor will maintain a deployment checklist to capture lessons learned, to be shared with State staff.
- f) Describe how the Vendor will perform an initial “smoke test” of the Crossroads system, including the batch and report cloud servers, prior to informing the State that the deployment is complete. Describe how the Vendor will obtain prior written approval from the State regarding restoring the backups of the application and databases should there be a critical system failure identified during smoke testing.
- g) Describe how the Vendor will provide for each build via secure FTP:
 - 1. An ISO image of the complete, cumulative source code, including instructions and prerequisites required to compile and produce executable code;
 - 2. A ZIP file (compatible with the pkware standard) of the executable code and installation scripts used by the Vendor during the install, database scripts applicable to the database server, and reports for the report server that was implemented. Describe the process for how this code and scripts can be utilized on any of the supported State environments.
- h) Describe how the Vendor will provide release notes and a refreshed environment summary matrix showing the level of Crossroads installed in each environment. Describe how the release notes will contain at a minimum:
 - 1. The Build Number.
 - 2. A detailed description of new Change Requests delivered in the build.
 - 3. A detailed description of any new Reports delivered in the build.
 - 4. A complete description of all defect corrections, including the defect reporting number(s), delivered in the build. This list will be separated by defects reported in Production, defects reported in Test, defects identified by the Vendor, and any permanent fix of any hotfixes previously applied to an environment.
 - 5. A complete list and description of any system tables added, changed or removed.
 - 6. A detailed description, including illustrations of affected system screens, of any corrective, adaptive, or perfective changes made by the Vendor to address issues found during QA efforts.
 - 7. All details needed for the State to accurately update automated performance testing scripts and other tools.
 - 8. Comments and additional information; and
 - 9. The audience for Release Notes is both State WIC staff and State IT. Notes will be written using non-technical IT language that can be understood by State WIC staff.
- i) Describe how the Vendor will email State staff at the start, as needed during installation, and at completion of each deployment.
- j) Describe how the The Environment Summary Matrix will be updated, listing the applicable defect reporting number(s), and provided to the State after any hotfix is applied to an environment.

- k) Describe how the Vendor will provide and maintain a complete installation and configuration guide, detailing how to perform fresh ground-up installs of the system on cloud servers and workstations.
- l) Describe in detail on how production installation services will be performed after Business hours, including all State, Federal, and Vendor holidays and weekends, as requested by the State. Production upgrades typically begin on Saturdays between 8:00 AM and 6:00 PM Eastern Time to minimize disruption to the NC local agencies, with day and time subject to change at the discretion of the State.

3.5.10 DEPLOYMENT OF RELEASES FOR STATEWIDE PRODUCTION

Describe Vendor's approach to providing the following services and tasks under this category.

- a) The Awarded Vendor will complete migration from the State-hosted production environment to the Vendor-managed cloud production environment before the end of the Transition-In Phase. This includes migration of all applications (WPF and portals), databases, and file system contents.
- b) How Vendor will provide a detailed Production Deployment Plan after contract execution that describes the procedures, detailed schedules, and resources needed to implement and immediately support each release of Crossroads statewide. The Plan will be submitted as stipulated in Table 1 – List of Product Deliverables.

A minimum of two hundred (200) hours of Change Requests and a minimum of twenty (20) defect corrections (or smaller minimums at the sole discretion of the State), will be developed, tested, and delivered for UAT along with its final UAT Readiness Report no later than ninety (90) Calendar Days from the start of the Maintenance and Enhancement Phase.

- c) Describe how the results of UAT and a walkthrough of the System will demonstrate that the System is functional and ready for statewide deployment in a production environment.
- d) Describe how the production environment will be seeded with necessary data that will be used for statewide deployment and populating all necessary tables, etc., so that the System may be fully operational as sites encounter the new release in production.
- e) Describe and explain how the Vendor will coordinate with outside entities (WIC EBT Provider, etc.) to ensure that all interfaces and connectivity will be operational.
- f) Describe how the Vendor will participate with State staff to determine the deployment schedule.
- g) Describe how the Vendor will provide to the State updates to the following System documentation in a timely manner prior to deployment of each major system release to reflect all software Change Requests and defect corrections:
 1. Detailed Functional Design Documents (DFDD), including a detailed Risk Code Summary Matrix and Trigger Summary;
 2. User Manuals;
 3. Detailed Technical Specifications (DTS), including Data Dictionary (currently available in Compiled HTML (CHM) format) and a detailed listing of all System Tables;
 4. Interface Control Document (ICD) for the WIC Universal MIS-EBT Interface (WUMEI);
 5. External Communication Documentation (ECD);

6. Report Definition Documentation (RDD);
 7. Installation and Configuration Instructions, including hardware and software prerequisites;
 8. Central Processing Site Operations Manual;
 9. White Papers to provide written guidance to assist the State with understanding or solving an issue.
 10. The above System documentation will be maintained in Microsoft Office 365 format, that is editable by State staff, and provide all ancillary files used for the creation of embedded figures, diagrams, tables, or other non-editable components of the documentation.
- h) Describe how the Vendor will assist, at no additional cost, with the development of business rules and other guidance with North Carolina WIC to govern program operations.
 - i) Detail how the Vendor will support statewide deployment of release including the following:
 1. Monitoring end of day processing to ensure successful completion by the start of the next Business Day, taking corrective action as needed, and reporting the status to North Carolina WIC.
 2. Verifying that System housekeeping functions have been completed, taking corrective action as needed, and reporting the status to North Carolina WIC.
 3. Verifying that appropriate files have been sent to / received from the WIC EBT Provider and others, processed, taking corrective action as needed, and reporting the status to North Carolina WIC.
 4. Providing Help Desk support to State Office staff.
 - j) Describe and detail the error logging system that the Vendor will provide or monitor for implemented sites to log errors.
 - k) Describe and explain the process and timeline to fix all errors in a timely fashion to allow rapid retesting to verify that the errors have been corrected. Describe how all Critical Component Failure and Major Component Failure severity errors will be corrected within the time provided in the SLA. Describe how all identified defects will be corrected before the System can be certified as ready for Statewide Deployment. Exceptions may be granted if the State determines that there are sufficient alternative processes in place to mitigate the effects of the defect.
 - l) Describe how the Vendor will provide in the Deployment Plan the procedures for application and database rollback in the event of a significant release failure in the production environment. Describe the procedures for preserving new production data that would otherwise be lost following a database rollback.

3.5.11 SYSTEM TRAINING

Describe Vendor's approach for training all State staff that will participate in a release UAT onsite in North Carolina, if requested by the State.

3.5.12 SYSTEM CHANGE REQUEST PROCESS

Describe Vendor's approach for completing System enhancements and modifications to improve the operation or functionality of the System, to comply with new Federal regulations or requirements, to comply with changes in State policy and procedure, or to meet other corrective, adaptive, or perfective needs via work authorization / supplemental hours. This process applies only to enhancements and modifications to the Crossroads system.

- a) The following services and tasks are required under this category at no additional cost to the State. **These specifications do not constitute or imply any promise or intention for the State to fund or approve Change Requests.** Adhering to the prescribed Change Request process as follows:
1. Explain how the Vendor can review the CR Concept, ask for clarifications when needed, identify associated risks with the CR Concept when appropriate and then prepare a CR Response fifteen (15) Calendar Days of receipt of the CR Concept for State review and approval within. The CR Response will include the Vendor's understanding of the original CR Concept with high-level detail like content provided in the original CR Concept, and a high-level non-binding system design outlining what Crossroads functions and screens are affected and conceptual estimate of hours and cost.
 2. Explain how the State can review, modify and approve the CR Response as appropriate and notify the Vendor. The Vendor will then prepare a detailed system design document and binding hour and cost estimates (CR Draft Estimate) within fifteen (15) Calendar Days of receipt of the State approval of the CR Response, or within thirty (30) Calendar Days of the State's approval of a CR Response which the Vendor estimates will require three hundred (300) hours or more to complete (Major CR).
 3. Explain how the State can review the CR Draft Estimate and notify the Vendor within thirty (30) Calendar Days, or longer if USDA/FNS approval of the CR Draft Estimate is required, that is approved, requires further rework, put on hold, or withdrawn. Approved CR Draft Estimates will be signed by the State and returned to the Vendor. The Vendor will then sign and return the CR Draft Estimate to the State.
 4. Explain how the Vendor can offer and coordinate cost sharing of common code changes among any other WIC States where the Vendor maintains and enhances any version of Crossroads or similar functionality that can be used across the Vendor's MIS offerings.
 5. Explain how the Vendor can obtain mutual agreement with the State on a deployment schedule for approved CR Estimates that considers the urgency of the change and the need to meet Federal deployment deadlines as appropriate.
 - i. Explain how approved changes requiring less than three hundred (300) hours can be developed, tested and delivered for UAT within sixty (60) Calendar Days of State approval of the CR Draft Estimate, and how approved changes requiring three hundred (300) hours or more can be developed, tested and delivered for UAT within ninety (90) Calendar Days of State approval of the CR Draft Estimate.
 - ii. Explain how the Vendor has the staff, equipment, and all other resources to develop and test approximately one hundred fifty (150) hours of approved Change Requests per quarter, if requested by the State. Explain how the Vendor will address situations where more hours are required.

- b) Changes to reference tables are not billable changes but are normal system maintenance activities covered at no additional cost. Reference table changes will still be initiated by a CR from the State and a corresponding CR Response from the Vendor but will not require the detailed system design document unless the CR affects existing System Documentation.

The Vendor will be responsible for making all reference table changes within five (5) Calendar Days of State approval of the CR Response.

- c) Changes to the System that are outside of the scope of this RFP, the Vendor's proposal, and the existing Crossroads Detailed Functional Design Documentation will be considered for additional cost and will go through the full change request process described above.
- d) Changes to the EBT interface, including FMNP, will be implemented by the Vendor at no additional cost to the State. Such changes will be initiated by a CR Concept from the State and a corresponding CR Response and CR Draft Estimate from the Vendor, provided however that such CR Draft Estimate will be at no cost to the State.
- e) Describe at least three (3) change request items, from the Vendor's experience, that the Vendor has implemented. Describe creative opportunities and best practices that will minimize or mitigate change requests and potential costs associated with change requests, such as cost sharing with other State WIC Programs that may be contracted with the Vendor.
- f) Corrections / defect fixes to correct deficiencies based on the most recently updated published System design documentation (or implemented CRs/estimates where documentation has not yet been updated) are subject to the change request process but at no additional cost.
- g) The Vendor will provide to the State timely updates to appropriate System documentation.
- h) Describe the Vendor's process to ensure that appropriate documentation is updated in a timely manner as software changes occur.
- i) Describe the Vendor's process to log and track the status of pending CRs including:
 - 1. The State and Vendor will mutually agree on an assigned sequence number;
 - 2. A short description of the requested change;
 - 3. Whether the change is a table change, code change, or other;
 - 4. The date of the original CR from the State;
 - 5. The date the CR Response was sent to the State;
 - 6. The date the CR Response was approved/not approved by the State;
 - 7. The date the CR Estimate was submitted to the State;
 - 8. The date the CR Estimate was approved/not approved/put on hold by the State;
 - 9. The binding hours and cost of the change;
 - 10. The proposed delivery date for UAT of the completed Change Request;
 - 11. Comments section;
 - 12. Current version of any associated documents;
- j) For those Change Requests that are at additional cost to be paid by the State, the Vendor's invoice will be processed for payment upon completion and delivery of the Change Request and acceptance of the delivered Change Request by the State. The amount paid for Change

Requests will be based on the amount contained in the CR Draft Estimate, signed by the State and the Vendor.

The State will have the option to defer acceptance of a Change Request until the change has been implemented in production, and all required defect corrections found against the Change Request in production have been subsequently implemented into production.

3.5.13 TECHNICAL UPGRADES AND ENVIRONMENT VALIDATION

Describe the Vendor's approach to recommending technology upgrades and providing environment compatibility / validation services. The services will include, but not be limited to upgrades to hardware infrastructure, operating systems including web browser, database management systems, and other cloud server or workstation software and hardware to maintain supportable non-production and production environments as third parties release new versions of products, or as current Crossroads components approach end-of-life. Describe how the Vendor will schedule third-party software patches and upgrades to all non-production and production environments through the DHHS Release Manager.

Describe how the Vendor will:

1. Provide annual written recommendations for upgrades to maintain the Crossroads system and third-party software components, at a version supported by the software vendor and in conformance with North Carolina security and architectural standards. This recommendation will be presented onsite by the Vendor in Raleigh, NC if requested by the State.
2. Proactively test and validate the Crossroads system for use with the latest release of relevant hardware and software technologies. The testing results and inventory of validated hardware and software will be maintained in the existing System Documentation. Examples of hardware and software to consider include, but are not limited to:
 1. Hardware
 - a. Scanners;
 - b. Workstation Printers;
 - c. Signature Pads;
 - d. Bar Code Scanners;
 - e. Label Writers;
 - f. EBT Card Readers;
 - g. Lab Equipment such as weight scales, etc.;
 - h. RAM memory requirements, for workstations;
 - i. Disk space requirements for workstations;
 - j. Graphics card requirements
 2. Software
 - a. Operating Systems, such as Windows;
 - b. Web Browsers, such as Microsoft Edge;
 - c. Database Management Systems, such as SQL Server;
 - d. .NET Framework and other middleware;

- e. Web server components;
- f. Adobe products;
- g. Microsoft Office products;
- h. Software Drivers for above Hardware;
- i. Telehealth frameworks for WIC participant experience

3.5.14 CONTRACT TRANSITION-OUT PROCEDURES

In the event of Contract termination for any reason, non-renewal by the State, or at the expiration of the Contract, the Vendor will be required to provide transition assistance.

Describe a detailed Transition-Out Plan for State review and acceptance, that describes the procedures, detailed schedules, and resources needed to successfully transition services to a new MIS Vendor. Specifications are listed below, in addition to Attachment B: Department of Information Technology Terms and Conditions.

Describe Vendor's Transition-Out Completion Report addressing:

- a) Providing an export of all regression and performance test artifacts, including but not limited to test scripts, test cases, test scenarios, etc.
- b) Providing a final copy of all source code software, compilation instructions and tools and final updated documentation.
- c) Providing an export of all issues and file attachments contained in the issue reporting system.
- d) Providing an export of all action items contained in the action item tracking tool.
- e) Providing an export of all finalized CR documents, including sample documents and templates that the Vendor has used for the Change Request Process.
- f) Returning all hardware and software that may be owned by the State upon request by the State. This includes system peripherals and other hardware.
- g) Maintaining the collaboration web site to allow State staff (or designee) to download artifacts until the Contract expires or is terminated.
- h) Ensuring that appropriate Vendor development, test, business analyst and other help desk staff are retained until expiration or termination of the Contract.
- i) Providing technical training to the State (and/or its designee) for eighty (80) hours to include a thorough overview of the system design, including a detailed walkthrough of the source code if requested, at a location to be determined by the State including the incumbent Vendor's facilities. Any unused Supplemental Service Hours may be utilized to provide additional training above these eighty (80) hours if requested by the State. These eighty (80) hours will not include preparation time by the Vendor, or travel time for Vendor staff.
- j) Describe how the Vendor will assure and confirm that any data or system design provided by or for the State remains the property of the State and may not be marketed or sold by the Vendor without the express written consent of the State.
- k) Until the Vendor has certified the completion of the data destruction or purge, describe how the Vendor will continue to comply with all data security sections within this RFP, even after the Contract has terminated or expired.

- l) Describe how Vendor will export or migrate (at the sole discretion of the State) all data (including file systems) from all production and non-prod environments into new environments to be determined by the State.
- m) Describe Vendor's approach to preserving the State's data in the Crossroads 3rd party cloud infrastructure and transferring the Vendor's PaaS or similar service model to the State or its designee, (which the State may request in its sole discretion).

3.5.15 NORTH CAROLINA WIC PROGRAM AND FMNP PROGRAM DATA

Describe how the Vendor's proposal can accommodate the following volumes of data:

- a) The information in the table below provides a high-level overview of WIC Program demographics.

Table 5 - North Carolina WIC General Program Statistics

State Specific Workload Data	Estimated Values as of April 2024
Approximate number of participants per year	235,000
Approximate number of households per year	144,000
Approximate number of Local Agencies including EBCI	86
Approximate number of individual sites	170
Approximate number of State level users	40
Approximate number of local agency/clinic level users	1400
Average number of concurrent users, to be used for performance testing estimates	1000
Approximate number of active Authorized WIC Retail Vendor locations	1600

- b) The information in the table below provides an overview of the peer group breakdown for North Carolina vendors.

Table 6 - North Carolina WIC Retailer Peer Groups

Store Type	Location	Store Class Description	Approximately Number of Vendors in Peer Group as of March 2024
Pharmacy	Statewide	Free-standing pharmacy that sells a limited variety of foods	283
Convenience Store	Statewide	Retailer with a limited assortment of grocery items	31
Mass Merchandiser and Commissary	Statewide	Retailer that sells a wide variety of merchandise but also carries groceries and has store locations in most or all states. Grocery store operated by US Defense Commissary on a military base	233
Independent Grocery	Urban	Retailer that primarily sells groceries with fewer than 11 store locations	112
Independent Grocery	Non-urban	Retailer that primarily sells groceries with fewer than 11 store locations	70
Regional Grocery Chain	Urban	Retailer that primarily sells groceries with at least 11 store locations and operates in 2 or more states	680
Regional Grocery Chain	Non-urban	Retailer that primarily sells groceries with at least 11 store locations and operates in 2 or more states	224

- c) The information in the table below provides a high-level overview of the FMNP process that was used for the 2024 season. NC moved to an electronic-based process for the 2024 season. .

Table 7 - North Carolina FMNP General Program Statistics

State Specific Workload Data	Estimated Values as of September 2024
Approximate number of participants per season	8200
Approximate number of cards issued per season	8200
Approximate number of counties in program	18
Approximate number of authorized farmers	100
Approximate number of farmers' markets	25

3.5.16 SUPPLEMENTAL SERVICES

Provide pricing for Supplemental Service Hours using Attachment D: Cost Form, Cost Table 7: Supplemental Hours, which will be used to document work authorizations via Change Requests to the Crossroads system that are for the account of the State.

The State will allocate up to thirty-five hundred (3500) Supplemental Service Hours Contract Years 1-7 (plus up to an additional five hundred (500) hours for each optional year, if applicable and at the State's discretion) until the end of the Contract term. Unused hours will carry forward to the next year, including optional years that become part of the contract term. Any Change Requests that require more than the Contract's remaining Supplemental Service Hours to complete will be made effective through the Parties' execution of a Contract amendment, implemented in compliance with the rules and practices of DIT Statewide Procurement.

1. Supplemental Service Hours: The aggregate of total Supplemental Service Hours for the entire Contract term will be available to the State beginning in Year 1.
2. Describe the process the Vendor would use for tracking Supplemental Service Hours allocated and expended.
3. Hours for Change Requests required to be performed at no additional cost to the State will not be expended from the Supplemental Services Hours.

4.0 COST OF VENDOR'S OFFER

4.1 OFFER COSTS

The Vendor must list, itemize, and describe any applicable offer costs in ATTACHMENT D: COST FORM.

4.2 PAYMENT SCHEDULE

- a) Signed invoices will be submitted electronically to this email address:
NSBContracts@dhhs.nc.gov
- b) Invoices for delivered change requests should only be submitted once the State has approved a deliverable as acceptable.
Invoices for ongoing maintenance and hosting will be submitted monthly and will bear the correct purchase order number to ensure prompt payment. The Vendor's failure to include the correct purchase order number may cause delay in payment.

To ensure that the Crossroads Vendor provides uninterrupted services to the State, WIC Participants, and WIC Retailers and meets the performance standards set forth in USDA FNS regulations, in this RFP and the SLA, North Carolina will establish a set of Crossroads system and service performance standards. It is the intent of the State that in the event of the Crossroads Vendor's failure to perform as provided in the USDA FNS regulations, in this RFP and the SLA, including during the Transition-Out period, the payment due the Crossroads Vendor may be reduced as documented in the SLA.

- c) Invoices will itemize the work for which payment is sought, and will include the deliverable # and agreed upon cost. Invoices can contain multiple deliverables, with an aggregated total cost.
- d) The State will make monthly payments to the Vendor for services rendered during the previous calendar month. The Vendor will provide an electronic copy of the monthly invoice signed by designated authorities.

5.0 EVALUATION

N.C.G.S §143B-1350(h): All offers are subject to evaluation of the most advantageous offer to the State. Evaluation shall include best value, as the term is defined in N.C.G.S. 143-135.9(a)(1), compliance with information technology project management policies, compliance with information technology security standards and policies, substantial conformity with the specifications, and other conditions set forth in the solicitation.

5.1 SOURCE SELECTION

A one step trade-off method of source selection will be utilized in this procurement to allow the State to award this RFP to the Vendor providing the Best Value and recognizing that Best Value may result in award other than the lowest price or highest technically qualified offer. By using this method, the overall ranking may be adjusted up or down when considered with or traded-off against other non-price factors.

- a) Evaluation Process Explanation. State Agency employees will review all offers. All offers will be initially classified as being responsive or non-responsive. If an offer is found non-responsive, it will not be considered further. All responsive offers will be evaluated based on stated evaluation criteria. Any references in an answer to another location in the RFP materials or Offer shall have specific page numbers and sections stated in the reference.
- b) To be eligible for consideration, Vendor's offer must substantially conform to the intent of all specifications. Compliance with the intent of all specifications will be determined by the State. Offers that do not meet the full intent of all specifications listed in this RFP may be deemed deficient. Further, a serious deficiency in the offer to any one (1) factor may be grounds for rejection regardless of overall evaluation.
- c) The evaluation committee may request clarifications, an interview with or presentation from any or all Vendors as allowed by 9 NCAC 06B.0307. However, the State may refuse to accept, in full or partially, the response to a clarification request given by any Vendor. Vendors are cautioned that the evaluators are not required to request clarifications; therefore, all offers should be complete and reflect the most favorable terms. Vendors should be prepared to send qualified personnel to Raleigh, North Carolina, to discuss technical and contractual aspects of the offer, if requested.
- d) Vendors are advised that the State is not obligated to ask for or accept, after the closing date for receipt of offer, data that is essential for a complete and thorough evaluation of the offer.

5.2 EVALUATION CRITERIA

Evaluation shall include best value, as the term is defined in N.C.G.S. § 143-135.9(a)(1), compliance with information technology project management policies as defined by N.C.G.S. §143B-1340, compliance with information technology security standards and policies, substantial conformity with the specifications, and other conditions set forth in the solicitation. The following Evaluation Criteria are listed in Order of Importance.

- 1) How well the Vendor's offer conforms with the specifications
- 2) How each Vendor's offer compares with other Vendors' offers
- 3) Total Cost of Ownership
- 4) Vendor Schedule / Timeline for completing work
- 5) Strength of references relevant or material to technology area(s) or Specifications and Vendor Past Performance (The Vendor may be disqualified from any evaluation or award if the Vendor or any key personnel proposed, has previously failed to perform satisfactorily during the performance of any contract with the State, or violated rules or statutes applicable to public bidding in the State)
- 6) Risks associated with Vendor's offer which include Vendor errata and exceptions.

5.3 BEST AND FINAL OFFERS (BAFO)

The State may establish a competitive range based upon evaluations of offers, and request BAFOs from the Vendor(s) within this range; e.g. "Finalist Vendor(s)". If negotiations or subsequent offers are solicited, the Vendor(s) shall provide BAFO(s) in response. Failure to deliver a BAFO when requested shall disqualify the non-responsive Vendor from further consideration. The State will evaluate BAFO(s), oral presentations, and product demonstrations as part of the Vendors' respective offers to determine the final rankings.

5.4 POSSESSION AND REVIEW

During the evaluation period and prior to award, possession of the bids and accompanying information is limited to personnel of the issuing agency, and to the committee responsible for participating in the evaluation. Vendors who attempt to gain this privileged information, or to influence the evaluation process (i.e. assist in evaluation) will be in violation of purchasing rules and their offer will not be further evaluated or considered.

After award of contract the complete bid file will be available to any interested persons with the exception of trade secrets, test information or similar proprietary information as provided by statute and rule. Any proprietary or confidential information, which conforms to exclusions from public records as provided by N.C.G.S. §132-1.2 must be clearly marked as such in the offer when submitted.

6.0 VENDOR INFORMATION AND INSTRUCTIONS

6.1 GENERAL CONDITIONS OF OFFER

6.1.1 VENDOR RESPONSIBILITY

It shall be the Vendor's responsibility to read this entire document, review all enclosures and attachments, and comply with all specifications, requirements and the State's intent as specified herein. If a Vendor discovers an inconsistency, error or omission in this solicitation, the Vendor should request a clarification from the State's contact person.

The Vendor will be responsible for investigating and recommending the most effective and efficient solution. Consideration shall be given to the stability of the proposed configuration and the future direction of technology, confirming to the best of its ability that the recommended approach is not short lived. Several approaches may exist for hardware configurations, other products and any

software. The Vendor must provide a justification for their proposed hardware, product and software solution(s) along with costs thereof. Vendors are encouraged to present explanations of benefits and merits of their proposed solutions together with any accompanying Services, maintenance, warranties, value added Services or other criteria identified herein.

6.1.2 RIGHTS RESERVED

While the State has every intention to award a contract as a result of this RFP, issuance of the RFP in no way constitutes a commitment by the State of North Carolina, or the procuring Agency, to award a contract. Upon determining that any of the following would be in its best interests, the State may:

- a) waive any formality;
- b) amend the solicitation;
- c) cancel or terminate this RFP;
- d) reject any or all offers received in response to this RFP;
- e) waive any undesirable, inconsequential, or inconsistent provisions of this RFP;
- f) if the response to this solicitation demonstrate a lack of competition, negotiate directly with one or more Vendors;
- g) not award, or if awarded, terminate any contract if the State determines adequate State funds are not available; or
- h) if all offers are found non-responsive, determine whether Waiver of Competition criteria may be satisfied, and if so, negotiate with one or more known sources of supply.

6.1.3 SOLICITATION AMENDMENTS OR REVISIONS

Any and all amendments or revisions to this document shall be made by written addendum from the Agency Procurement Office. If either a unit price or extended price is obviously in error and the other is obviously correct, the incorrect price will be disregarded.

6.1.4 ORAL EXPLANATIONS

The State will not be bound by oral explanations or instructions given at any time during the bidding process or after award. Vendor contact regarding this RFP with anyone other than the State's contact person may be grounds for rejection of said Vendor's offer. Agency contact regarding this RFP with any Vendor may be grounds for cancellation of this RFP.

6.1.5 E-PROCUREMENT

This is an E-Procurement solicitation. See ATTACHMENT B, paragraph #38 of the attached North Carolina Department of Information Technology Terms and Conditions.

The Terms and Conditions made part of this solicitation contain language necessary for the implementation of North Carolina's statewide E-Procurement initiative. It is the Vendor's responsibility to read these terms and conditions carefully and to consider them in preparing the offer. By signature, the Vendor acknowledges acceptance of all terms and conditions including those related to E-Procurement.

- a) General information on the E-Procurement service can be found at <http://eprocurement.nc.gov/>
- b) Within two days after notification of award of a contract, the Vendor must register in NC E-Procurement @ Your Service at the following website: <http://eprocurement.nc.gov/Vendor.html>

- c) As of the RFP submittal date, the Vendor must be current on all E-Procurement fees. If the Vendor is not current on all E-Procurement fees, the State may disqualify the Vendor from participation in this RFP.

6.1.6 ELECTRONIC VENDOR PORTAL (EVP)

The State has implemented the electronic Vendor Portal (eVP) that allow the public to retrieve award notices and information on the Internet at <https://evp.nc.gov>. Results may be found by searching by Solicitation Number or agency name. This information may not be available for several weeks dependent upon the complexity of the acquisition and the length of time to complete the evaluation process.

6.1.7 PROTEST PROCEDURES

Protests of awards exceeding \$25,000 in value must be submitted to the issuing Agency at the address given on the first page of this document. Protests must be received in the purchasing agency's office within fifteen (15) calendar days from the date of this RFP award and provide specific reasons and any supporting documentation for the protest. **All protests are governed by Title 9, Department of Information Technology (formerly Office of Information Technology Services), Subchapter 06B Sections .1101 - .1121.**

6.2 GENERAL INSTRUCTIONS FOR VENDOR

6.2.1 SITE OR PRE-OFFER CONFERENCE (RESERVED)

6.2.2 QUESTIONS CONCERNING THE RFP

All inquiries regarding the solicitation specifications or requirements are to be addressed to the contact person listed on Page One of this solicitation via the Ariba Sourcing Tool's message board. Vendor contact regarding this Solicitation with anyone other than the contact person listed on Page One of this Solicitation may be grounds for rejection of said Vendor's offer.

Written questions concerning this Solicitation will be received until **January 6, 2025 at 2:00 pm** Eastern Time.

They must be submitted to the contact person listed on Page One of this Solicitation via the Ariba Sourcing Tool's message board. Please enter "Questions Solicitation 30-25002-DCFW" as the subject for the message.

REFERENCE	VENDOR QUESTION
RFP Section, Page Number	

6.2.3 ADDENDUM TO RFP

If a pre-offer conference is held or written questions are received prior to the submission date, an addendum comprising questions submitted and responses to such questions, or any additional terms deemed necessary by the State shall become an Addendum to this RFP and provided via the State's Ariba Sourcing Tool. Vendors' questions posed orally at any pre-offer conference must be reduced to writing by the Vendor and provided to the Purchasing Officer as directed by said Officer. Oral answers are not binding on the State.

Critical updated information may be included in these Addenda. It is important that all Vendors bidding on this RFP periodically check the State's Sourcing Tool for all Addenda that may be issued prior to the offer opening date.

6.2.4 COSTS RELATED TO OFFER SUBMISSION

Crossroads WIC MIS 30-25002-DCFW

Costs for developing and delivering responses to this RFP and any subsequent presentations of the offer as requested by the State are entirely the responsibility of the Vendor. The State is not liable for any expense incurred by the Vendors in the preparation and presentation of their offers.

All materials submitted in response to this RFP become the property of the State and are to be appended to any formal documentation, which would further define or expand any contractual relationship between the State and the Vendor resulting from this RFP process.

6.2.5 VENDOR ERRATA AND EXCEPTIONS

Any errata or exceptions to the State's requirements and specifications may be presented on a separate page labeled "Exceptions to Requirements and Specifications". Include references to the corresponding requirements and specifications of the Solicitation. Any deviations shall be explained in detail. **The Vendor shall not construe this paragraph as inviting deviation or implying that any deviation will be acceptable. Offers of alternative or non-equivalent goods or services may be rejected if not found substantially conforming; and if offered, must be supported by independent documentary verification that the offer substantially conforms to the specified goods or services specification.** If a vendor materially deviates from RFP requirements or specifications, its offer may be determined to be non-responsive by the State.

Offers conditioned upon acceptance of Vendor Errata or Exceptions may be determined to be non-responsive by the State.

6.2.6 ALTERNATE OFFERS

The Vendor may submit alternate offers for various levels of service(s) or products meeting specifications. Alternate offers must specifically identify the RFP specifications and advantage(s) addressed by the alternate offer. Any alternate offers must be clearly marked with the legend as shown herein. Each offer must be for a specific set of Services or products and offer at specific pricing. If a Vendor chooses to respond with various service or product offerings, each must be an offer with a different price and a separate RFP offer. Vendors may also provide multiple offers for software or systems coupled with support and maintenance options, provided, however, all offers must satisfy the specifications.

Alternate offers must be submitted in a separate document and clearly marked "Alternate Offer for 'name of Vendor'" and numbered sequentially with the first offer if separate offers are submitted.

6.2.7 MODIFICATIONS TO OFFER

An offer may not be unilaterally modified by the Vendor.

6.2.8 BASIS FOR REJECTION

Pursuant to 9 NCAC 06B.0401, the State reserves the right to reject any and all offers, in whole or in part; by deeming the offer unsatisfactory as to quality or quantity, delivery, price or service offered; non-compliance with the specifications or intent of this solicitation; lack of competitiveness; error(s) in specifications or indications that revision would be advantageous to the State; cancellation or other changes in the intended project, or other determination that the proposed specification is no longer needed; limitation or lack of available funds; circumstances that prevent determination of the best offer; or any other determination that rejection would be in the best interest of the State.

6.2.9 NON-RESPONSIVE OFFERS

Vendor offers will be deemed non-responsive by the State and will be rejected without further consideration or evaluation if statements such as the following are included:

- "This offer does not constitute a binding offer",
- "This offer will be valid only if this offer is selected as a finalist or in the competitive range",
- "The Vendor does not commit or bind itself to any terms and conditions by this submission",

- “This document and all associated documents are non-binding and shall be used for discussion purposes only”,
- “This offer will not be binding on either party until incorporated in a definitive agreement signed by authorized representatives of both parties”, or
- A statement of similar intent

6.2.10 VENDOR REGISTRATION WITH THE SECRETARY OF STATE

Vendors do not have to be registered with the NC Secretary of State to submit an offer; however, in order to receive an award/contract with the State, they must be registered. Registration can be completed at the following website: https://www.sosnc.gov/Guides/launching_a_business

6.2.11 VENDOR REGISTRATION AND SOLICITATION NOTIFICATION SYSTEM

The NC electronic Vendor Portal (eVP) allows Vendors to electronically register with the State to receive electronic notification of current procurement opportunities for goods and Services available at the following website: <https://evp.nc.gov>.

This RFP is available electronically on the electronic Vendor Portal (eVP) at the following website: <https://evp.nc.gov>.

6.3 INSTRUCTIONS FOR OFFER SUBMISSION

6.3.1 GENERAL INSTRUCTIONS FOR OFFER

Vendors are strongly encouraged to adhere to the following general instructions in order to bring clarity and order to the offer and subsequent evaluation process:

- Organize the offer in the exact order in which the specifications are presented in the RFP. The Execution page of this RFP must be placed at the front of the Proposal. Each page should be numbered. The offer should contain a table of contents, which cross-references the RFP specification and the specific page of the response in the Vendor's offer.
- Provide complete and comprehensive responses with a corresponding emphasis on being concise and clear. Elaborate offers in the form of brochures or other presentations beyond that necessary to present a complete and effective offer are not desired.
- Clearly state your understanding of the problem(s) presented by this RFP including your proposed solution's ability to meet the specifications, including capabilities, features, and limitations, as described herein, and provide a cost offer.
- Supply all relevant and material information relating to the Vendor's organization, personnel, and experience that substantiates its qualifications and capabilities to perform the Services and/or provide the goods described in this RFP. If relevant and material information is not provided, the offer may be rejected from consideration and evaluation.
- Furnish all information requested; and if response spaces are provided in this document, the Vendor shall furnish said information in the spaces provided. Further, if required elsewhere in this RFP, each Vendor must submit with its offer sketches, descriptive literature and/or complete specifications covering the products offered. References to literature submitted with a previous offer will not satisfy this provision. Proposals that do not comply with these instructions may be rejected.
- Any offer that does not adhere to these instructions may be deemed non-responsive and rejected on that basis.
- Only information that is received in response to this RFP will be evaluated.** Reference to information previously submitted or Internet Website Addresses (URLs) will not suffice as a response to this solicitation.

6.3.2 OFFER ORGANIZATION

Within each section of its offer, Vendor should address the items in the order in which they appear in this RFP. Forms, attachments or exhibits, if any provided in the RFP, must be completed and included in the appropriate section of the offer. All discussion of offered costs, rates, or expenses must be presented in Section 4.0. Cost of Vendor's Offer.

The offer should be organized and indexed in the following format and should contain, at a minimum, all listed items below.

- a) Signed Execution Page AND all pages of this solicitation document in ONE (1) PDF. This includes:
 1. Attachments A and B
 2. Completed Description of Vendor Submitting Offer Form (Attachment C)
 3. Completed Cost Form of Vendor's Offer (Attachment D)
 4. Completed and Signed Vendor Certification Form (Attachment E)
 5. Completed Location of Workers Utilized by Vendor Form (Attachment F)
 6. Completed References (Attachment G)
 7. Completed Financial Statements (Attachment H)
 8. Attachment K
- b) Vendor Response to Specifications and Requirements
- c) Security Vendor Readiness Assessment Report (VRAR)
- d) Architecture Diagrams
- e) Detailed Project Timeline
- f) Errata and Exceptions if any
- g) Vendor's License and Maintenance Agreements if any
- h) Vendor may attach other supporting materials that it feels may improve the quality of its response. These materials should be included as items in a separate appendix.

6.3.3 OFFER SUBMITTAL

Due Date: **March 6, 2025**

Time: **2:00 pm** Eastern Time

IMPORTANT NOTE: It is the Vendor's sole responsibility to upload their offer to the Ariba Sourcing Module by the specified time and date of opening. Vendor shall bear the risk for late electronic submission due to unintended or unanticipated delay, including but not limited to internet issues, network issues, local power outages, or application issues. Vendor must include all the pages of this solicitation in their response.

Sealed offers, subject to the conditions made a part hereof, will be received until **2:00pm** Eastern Time on the day of opening and then opened, for furnishing and delivering the commodity as described herein. Offers must be submitted via the Ariba Sourcing Module with the Execution page signed and dated by an official authorized to bind the Vendor's firm. Failure to return a signed offer shall result in disqualification.

Attempts to submit a proposal via facsimile (FAX) machine, telephone, email, email attachments, or in any hardcopy format in response to this Bid SHALL NOT be accepted and will automatically be deemed Non-Responsive.

- a) Submit **one (1) signed, original electronic offer** through the Ariba Sourcing Module.
- b) The Ariba Sourcing Module document number is: WS1181143716
- c) All File names should start with the Vendor name first, in order to easily determine all the files to be included as part of the vendor's response. For example, files should be named as follows: Vendor Name-your file name.
- d) File contents **SHALL NOT** be password protected, the file formats must be in .PDF, .JPEG, .DOC or .XLS format, and shall be capable of being copied to other sources. Inability by the State to open the Vendor's files may result in the Vendor's offer(s) being rejected as Non-Responsive.
- e) **If the vendor's proposal contains any confidential information (as defined in Attachment B, then the vendor must provide one (1) signed, original electronic offer and one (1) redacted electronic copy.**

For Vendor training on how to use the Ariba Sourcing Tool to view solicitations, submit questions, develop responses, upload documents, and submit offers to the State, Vendors should go to the following site: <https://eprocurement.nc.gov/training/vendor-training>

Questions or issues related to using the Ariba Sourcing Tool itself can be directed to the North Carolina eProcurement Help Desk at 888-211-7440, Option 2. Help Desk representatives are available Monday through Friday from 7:30 AM Eastern to 5:00 PM Eastern

7.0 OTHER REQUIREMENTS AND SPECIAL TERMS

7.1 VENDOR UTILIZATION OF WORKERS OUTSIDE OF U.S.

In accordance with N.C.G.S. §143B-1361(b), the Vendor must detail the manner in which it intends to utilize resources or workers in the RFP response. The State of North Carolina will evaluate the additional risks, costs, and other factors associated with such utilization prior to making an award for any such Vendor's offer.

Complete ATTACHMENT F - Location of Workers Utilized by Vendor and submit with your offer.

7.2 FINANCIAL STATEMENTS

The Vendor shall provide evidence of financial stability by returning with its offer 1) completed Financial Review Form (Attachment I), and 2) copies of Financial Statements as further described hereinbelow. As used herein, Financial Statements shall exclude tax returns and compiled statements.

- a) For a publicly traded company, Financial Statements for the past three (3) fiscal years, including at a minimum, income statements, balance sheets, and statement of changes in financial position or cash flows. If three (3) years of financial statements are not available, this information shall be provided to the fullest extent possible, but not less than one year. If less than 3 years, the Vendor must explain the reason why they are not available.
- b) For a privately held company, when certified audited financial statements are not prepared: a written statement from the company's certified public accountant stating the financial condition, debt-to-asset ratio for the past three (3) years and any pending actions that may affect the company's financial condition.

- c) The State may, in its sole discretion, accept evidence of financial stability other than Financial Statements for the purpose of evaluating Vendors' responses to this RFP. The State reserves the right to determine whether the substitute information meets the requirements for Financial Information sufficiently to allow the State to evaluate the sufficiency of financial resources and the ability of the business to sustain performance of this RFP award. Scope Statements issued may require the submission of Financial Statements and specify the number of years to be provided, the information to be provided, and the most recent date required.

7.3 FINANCIAL RESOURCES ASSESSMENT, QUALITY ASSURANCE, PERFORMANCE AND RELIABILITY

- a) Contract Performance Security. The State reserves the right to require performance guaranties pursuant to N.C.G.S. §143B-1340(f) and 09 NCAC 06B.1207 from the Vendor without expense to the State.
- b) Project Assurance, Performance and Reliability Evaluation – Pursuant to N.C.G.S. §143B-1340, the State CIO may require quality assurance reviews of Projects as necessary.

7.4 VENDOR'S LICENSE OR SUPPORT AGREEMENTS

Vendor should present its license or support agreements for review and evaluation. Terms offered for licensing and support of Vendors' proprietary assets will be considered.

The terms and conditions of the Vendor's standard services, license, maintenance or other agreement(s) applicable to Services, Software and other Products acquired under this RFP may apply to the extent such terms and conditions do not materially change the terms and conditions of this RFP. In the event of any conflict between the terms and conditions of this RFP and the Vendor's standard agreement(s), the terms and conditions of this RFP relating to audit and records, jurisdiction, choice of law, the State's electronic procurement application of law or administrative rules, the remedy for intellectual property infringement and the exclusive remedies and limitation of liability in the DIT Terms and Conditions herein shall apply in all cases and supersede any provisions contained in the Vendor's relevant standard agreement or any other agreement. The State shall not be obligated under any standard license and/or maintenance or other Vendor agreement(s) to indemnify or hold harmless the Vendor, its licensors, successors or assigns, nor arbitrate any dispute, nor pay late fees, penalties, legal fees or other similar costs.

7.5 RESELLERS (RESERVED)

7.6 DISCLOSURE OF LITIGATION

The Vendor's failure to fully and timely comply with the terms of this section, including providing reasonable assurances satisfactory to the State, may constitute a material breach of the Agreement.

- a) The Vendor shall notify the State in its offer, if it, or any of its subcontractors, or their officers, directors, or key personnel who may provide Services under any contract awarded pursuant to this solicitation, have ever been convicted of a felony, or any crime involving moral turpitude, including, but not limited to fraud, misappropriation or deception. The Vendor shall promptly notify the State of any criminal litigation, investigations or proceeding involving the Vendor or any subcontractor, or any of the foregoing entities' then current officers or directors during the term of the Agreement or any Scope Statement awarded to the Vendor.
- b) The Vendor shall notify the State in its offer, and promptly thereafter as otherwise applicable, of any civil litigation, arbitration, proceeding, or judgments against it or its subcontractors during the three (3) years preceding its offer, or which may occur during the term of any awarded to the Vendor pursuant to this solicitation, that involve (1) Services or related goods similar to those provided pursuant to any contract and that involve a claim that may affect the viability or financial stability of the Vendor, or (2) a claim or written allegation of fraud by the Vendor or any subcontractor hereunder,

arising out of their business activities, or (3) a claim or written allegation that the Vendor or any subcontractor hereunder violated any federal, state or local statute, regulation or ordinance. Multiple lawsuits and or judgments against the Vendor or subcontractor shall be disclosed to the State to the extent they affect the financial solvency and integrity of the Vendor or subcontractor.

- c) All notices under subsection A and B herein shall be provided in writing to the State within thirty (30) calendar days after the Vendor learns about any such criminal or civil matters; unless such matters are governed by the DIT Terms and Conditions annexed to the solicitation. Details of settlements which are prevented from disclosure by the terms of the settlement shall be annotated as such. Vendor may rely on good faith certifications of its subcontractors addressing the foregoing, which certifications shall be available for inspection at the option of the State.

7.7 CRIMINAL CONVICTION

In the event the Vendor, an officer of the Vendor, or an owner of a 25% or greater share of the Vendor, is convicted of a criminal offense incident to the application for or performance of a State, public or private Contract or subcontract; or convicted of a criminal offense including but not limited to any of the following: embezzlement, theft, forgery, bribery, falsification or destruction of records, receiving stolen property, attempting to influence a public employee to breach the ethical conduct standards for State of North Carolina employees; convicted under State or federal antitrust statutes; or convicted of any other criminal offense which in the sole discretion of the State, reflects upon the Vendor's business integrity and such vendor shall be prohibited from entering into a contract for goods or Services with any department, institution or agency of the State.

7.8 SECURITY AND BACKGROUND CHECKS

The Agency reserves the right to conduct a security background check or otherwise approve any employee or agent provided by the Vendor, and to refuse access to or require replacement of any such personnel for cause, including, but not limited to, technical or training qualifications, quality of work or change in security status or non-compliance with the Agency's security or other similar requirements.

All State and Vendor personnel that have access to data restricted by the State Security Manual and Policies must have a security background check performed. The Vendors are responsible for performing all background checks of their workforce and subcontractors. The State reserves the right to check for non-compliance.

7.9 ASSURANCES

In the event that criminal or civil investigation, litigation, arbitration or other proceedings disclosed to the State pursuant to this Section, or of which the State otherwise becomes aware, during the term of the Agreement, causes the State to be reasonably concerned about:

- a) the ability of the Vendor or its subcontractor to continue to perform the Agreement in accordance with its terms and conditions, or
- b) whether the Vendor or its subcontractor in performing Services is engaged in conduct which is similar in nature to conduct alleged in such investigation, litigation, arbitration or other proceedings, which conduct would constitute a breach of the Agreement or violation of law, regulation or public policy, then the Vendor shall be required to provide the State all reasonable assurances requested by the State to demonstrate that: the Vendor or its subcontractors hereunder will be able to continue to perform the Agreement in accordance with its terms and conditions, and the Vendor or its subcontractors will not engage in conduct in performing Services under the Agreement which is similar in nature to the conduct alleged in any such litigation, arbitration or other proceedings.

7.10 CONFIDENTIALITY OF OFFERS

All offers and any other RFP responses shall be made public as required by the NC Public Records Act and GS 143B-1350. Vendors may mark portions of offers as confidential or proprietary, after determining

that such information is excepted from the NC Public Records Act, provided that such marking is clear and unambiguous and preferably at the top and bottom of each page containing confidential information. Standard restrictive legends appearing on every page of an offer are not sufficient and shall not be binding upon the State.

Certain State information is not public under the NC Public Records Act and other laws. Any such information which the State designates as confidential and makes available to the Vendor in order to respond to the RFP or carry out the Agreement, or which becomes available to the Vendor in carrying out the Agreement, shall be protected by the Vendor from unauthorized use and disclosure. The Vendor shall not be required under the provisions of this section to keep confidential, (1) information generally available to the public, (2) information released by the State generally, or to the Vendor without restriction, (3) information independently developed or acquired by the Vendor or its personnel without reliance in any way on otherwise protected information of the State. Notwithstanding the foregoing restrictions, the Vendor and its personnel may use and disclose any information which it is otherwise required by law to disclose, but in each case only after the State has been so notified, and has had the opportunity, if possible, to obtain reasonable protection for such information in connection with such disclosure.

7.11 PROJECT MANAGEMENT

All project management and coordination on behalf of the Agency shall be through a single point of contact designated as the Agency Project Manager. The Vendor shall designate a Vendor Project Manager who will provide a single point of contact for management and coordination of the Vendor's work. All work performed pursuant to the Agreement shall be coordinated between the Agency Project Manager and the Vendor Project Manager.

7.12 MEETINGS

The Vendor is required to meet with Agency personnel, or designated representatives, to resolve technical or contractual problems that may occur during the term of the Agreement. Meetings will occur as problems arise and will be coordinated by Agency. The Vendor will be given reasonable and sufficient notice of meeting dates, times, and locations. Face to face meetings are desired. However, at the State's option and Vendor's expense, a conference call meeting or other virtual means may be substituted.

7.13 RECYCLING AND SOURCE REDUCTION

It is the policy of this State to encourage and promote the purchase of products with recycled content to the extent economically practicable, and to purchase items which are reusable, refillable, repairable, more durable, and less toxic to the extent that the purchase or use is practicable and cost-effective. We also encourage and promote using minimal packaging and the use of recycled/recyclable products in the packaging of goods purchased. However, no sacrifice in quality of packaging will be acceptable. The Vendor remains responsible for providing packaging that will protect the commodity and contain it for its intended use. Vendors are strongly urged to bring to the attention of the purchasers at the NCDIT Statewide IT Procurement Office those products or packaging they offer which have recycled content and that are recyclable.

7.14 SPECIAL TERMS AND CONDITIONS

- a) Should any of the Transition-Out Period tasks or the Transition-Out Completion Report not be completed and accepted by the State by the Contract end date, the Vendor will be assessed a one-time 5.00% liquidated damages of the Total Ten-Year Cost ("Liquidated Damages Assessment Amount") included in Cost Table 1. This Liquidated Damages Assessment Amount will be applied against any payments due to the Vendor. If all Vendor invoices have been paid at the time this Liquidated Damages Assessment Amount has been assessed, the Vendor will be required to pay the State this Liquidated Damages Assessment Amount within thirty (30) Calendar Days after receiving written notification of such assessment.

b) Paragraph #9 in Section 1 of the DIT Terms and Conditions is supplemented as follows: The Agency reserves the right to perform post-delivery and post-training acceptance testing for a period beginning at the start of the M&E Phase and lasting eight (8) weeks. The Agency also reserves the right to have an independent Vendor conduct testing pertaining to the functions, auditability, and related matters. At any time before the end of the test and assurance period the Agency may require any or all of the following:

- i) Have the Vendor modify the installed software to eliminate the deficiency to the Agency's satisfaction.
- ii) Have the Vendor re-install a new copy of the software product(s).
- iii) Extend the acceptance testing period for a period of ____30____ days to allow time for Vendor to remedy the problems.
- iv) Remove the application software, cancel this Agreement, and recover payments extended from Agency funds.

7.15 AGENCY TERMS AND CONDITIONS (RESERVED)

ATTACHMENT A: DEFINITIONS

- 1) **24x7:** A statement of availability of systems, communications, and/or supporting resources every hour (24) of each day (7 days weekly) throughout every year for periods specified herein. Where reasonable downtime is accepted, it will be stated herein. Otherwise, 24x7 implies NO loss of availability of systems, communications, and/or supporting resources.
- 2) **Cybersecurity Incident (GS 143B-1320):** An occurrence that:
 - a. Actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or
 - b. Constitutes a violation or imminent threat of violation of law, security policies, privacy policies, security procedures, or acceptable use policies.
- 3) **Deliverables:** Deliverables, as used herein, shall comprise all Hardware, Vendor Services, professional Services, Software and provided modifications to any Software, and incidental materials, including any goods, Software or Services access license, data, reports and documentation provided or created during the performance or provision of Services hereunder. Deliverables include “Work Product” and means any expression of Licensor’s findings, analyses, conclusions, opinions, recommendations, ideas, techniques, know-how, designs, programs, enhancements, and other technical information; but not source and object code or software.
- 4) **Goods:** Includes intangibles such as computer software; provided, however that this definition does not modify the definition of “goods” in the context of N.C.G.S. §25-2-105 (UCC definition of goods).
- 5) **NCDIT or DIT:** The NC Department of Information Technology.
- 6) **Open Market Contract:** A contract for the purchase of goods or Services not covered by a term, technical, or convenience contract.
- 7) **Reasonable, Necessary or Proper:** as used herein shall be interpreted solely by the State of North Carolina.
- 8) **Request for Proposal (RFP):** The RFP is a formal, written solicitation document typically used for seeking competition and obtaining offers for more complex services or a combination of goods and services. The RFP is used when the value is over \$10,000. This document contains specifications of the RFP, instructions to bidders and the standard IT Terms and Conditions for Goods and Related Services. User should add Supplemental Terms and Conditions for Software and Services, when applicable.
- 9) **Security Breach:** As defined in N.C.G.S. §75-61.
- 10) **Significant Security Incident (GS 143B-1320):** A cybersecurity incident that is likely to result in demonstrable harm to the State's security interests, economy, critical infrastructure, or to the public confidence, civil liberties, or public health and safety of the residents of North Carolina. A significant cybersecurity incident is determined by the following factors:
 - a. Incidents that meet thresholds identified by the Department jointly with the Department of Public Safety that involve information:
 - i. That is not releasable to the public and that is restricted or highly restricted according to Statewide Data Classification and Handling Policy; or
 - ii. That involves the exfiltration, modification, deletion, or unauthorized access, or lack of availability to information or systems within certain parameters to include (i) a specific threshold of number of records or users affected as defined in G.S. 75-65 or (ii) any additional data types with required security controls.

- b. Incidents that involve information that is not recoverable or cannot be recovered within defined time lines required to meet operational commitments defined jointly by the State agency and the Department or can be recovered only through additional measures and has a high or medium functional impact to the mission of an agency.

11) Vendor: Company, firm, corporation, partnership, individual, etc., submitting an offer in response to a solicitation.

12) Additional Defined Terms:

- a. **.NET Framework:** A Microsoft proprietary platform for building desktop, web, and mobile applications.
- b. **ASP.NET:** A server-side web-application framework designed for web development to produce dynamic web pages.
- c. **BFPC:** Breastfeeding Peer Counseling Program, a component of the Crossroads MIS system.
- d. **Central Processing Site:** The data center that hosts Crossroads environments.
- e. **ClickOnce technology:** A deployment technology that enables you to create self-updating Windows-based applications that can be installed and run with minimal user interaction.
- f. **CNSS:** Community Nutrition Services Section, an organization within NC DCFW.
- g. **CR:** Change Request, also known as a Change Order. A design document that describes desired enhancements to the Crossroads MIS system.
- h. **DFDD:** Detailed Functional Design Documents, documentation that defines the detailed business requirements for the Crossroads system.
- i. **DHHS:** The North Carolina Department of Health and Human Services.
- j. **Data Dictionary:** A component of the Detailed Technical Specifications, providing detailed information for each data element in the system.
- k. **Defect:** An error in coding or logic that causes the product to malfunction or to produce incorrect or unexpected results, as required by the DFDD or other regulations and agreements.
- l. **DTS:** Detailed Technical Specifications, documentation that describes various aspects of the system architecture.
- m. **Deployment:** Unless otherwise stipulated, this refers to the phase following completion of UAT, where the Vendor installs the accepted Crossroads release into production.
- n. **Development:** Unless otherwise stipulated, this refers to the phase before UAT, where the Vendor modifies and tests a Crossroads release with agreed maintenance and enhancements.
- o. **Documentation:** Unless otherwise stipulated, this refers to all Crossroads MIS documentation, including but not limited to Detailed Functional Design Documents (DFDD), User Manuals, Detailed Technical Specifications (DTS), Interface Control Documents (ICD), External Communication Documentation (ECD), Report Definition Documentation (RDD), Installation and Configuration Instructions, Central Processing Site Operations Manual, Environment Summary Matrix, Release Notes.
- p. **DCFW:** The Division of Child and Family Well-Being, an organization within NC DHHS.
- q. **EBCI:** Eastern Band of Cherokee Indians, a separate WIC State Agency that utilizes data processing services under the North Carolina Crossroads MIS system.
- r. **EBT:** Electronic Benefit Transfer. This technology allows WIC benefits to be issued and redeemed via magnetically encoded payment cards.
- s. **ECD:** External Communication Documentation, which describes system interfaces to third party systems.
- t. **Environment:** System components, such as servers and databases, on which an instance of the Crossroads software is installed.
- u. **Environment Summary Matrix:** Documentation that summarizes the various versions of software installed on each of the environments.
- v. **FMNP:** Farmers' Market Nutrition Program, a component of the Crossroads MIS system.

- w. **FNS:** Food and Nutrition Service, an agency within the United States Department of Agriculture.
- x. **Handbook 901:** FNS reference and guide for State Agencies that administer WIC programs.
- y. **Hotfix:** A software error correction applied to test or production environments, made quickly and outside of normal development and testing processes. Characterized as a patch, not a release.
- z. **ICD:** Interface Control Document, which describes the system interface to the WIC EBT Provider. Contains far greater detail than an ECD.
- aa. **ISO:** A single software file that contains an exact copy of an optical disk, such as a CD-ROM or DVD.
- bb. **IV&V:** Independent Verification and Validation
- cc. **JAD:** Joint Application Design, a process to collect business requirements.
- dd. **M&E:** Maintenance and Enhancement, the process for ongoing modifications of the Crossroads system after the completion of the initial design, development, and implementation contract.
- ee. **MIS:** Management Information System. The complete Crossroads solution serving WIC state and local offices, WIC retail vendors, WIC participants, and other external stakeholders.
- ff. **Microsoft SQL Server:** A relational database management system (RDBMS) that stores and retrieves data for other software applications
- gg. **Onsite:** All staff are physically present in the subject facilities. No stakeholder is participating via webinar, conference calls, or any other virtual method.
- hh. **RDD:** Report Definition Documentation, which defines data elements and report layouts.
- ii. **Release Notes:** Documentation that describes the details of all software changes, both enhancements and defect corrections, included in a software release.
- jj. **Service Model:** Various levels of computing outsourced to a cloud computing provider, such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS).
- kk. **SSL connection:** Secure Sockets Layer Connection. A communication protocol that creates a secure connection between two devices or applications on a network.
- ll. **Site and System Environment:** The Central Processing Site, and associated infrastructure and platform within the NC Department of Information Technology that hosts the Crossroads system, and the vendor-hosted cloud infrastructure.
- mm. **The State:** Is the State of North Carolina, and its Agencies.
- nn. **Storage Area Network (SAN):** A high-speed network that connects storage devices so that multiple servers and computers can access a shared pool of storage space.
- oo. **Transition-In:** Startup contract activities where the Vendor works with the current incumbent vendor to assume all M&E roles and responsibilities.
- pp. **Transition-Out:** Closeout contract activities where the Vendor transitions its incumbent M&E roles and responsibilities to a new vendor.
- qq. **UAT:** User Acceptance Testing, the phase after Development where the State evaluates the delivered Crossroads release, to determine if it is ready for Deployment.
- rr. **User Manual:** Documentation that describes system operation to end users.
- ss. **Vendor:** Company, firm, corporation, partnership, individual, etc., submitting an offer in response to a solicitation.
- tt. **WBS:** Work Breakdown Structure, a decomposition of the contract into phases, deliverables, and work packages.
- uu. **WIC:** The Supplemental Nutrition Program for Women, Infants, and Children, a federal assistance program provided by FNS.

- vv. **WPF:** The Microsoft technology that runs the Crossroads application on a Windows workstation
- ww. **WUMEI:** WIC Universal MIS-EBT Interface. The design documentation that describes the interface between Crossroads and the EBT Provider.
- xx. **XML-based Web Services:** An industry standard message format used in interfaces between applications.

ATTACHMENT B: DEPARTMENT OF INFORMATION TECHNOLOGY TERMS AND CONDITIONS FOR VENDOR HOSTED SOLUTIONS

Section 1. General Terms and Conditions Applicable to All Purchases

1) **DEFINITIONS:** As used herein;

Agreement means the contract awarded pursuant to this RFP.

Deliverable/Product Warranties shall mean and include the warranties provided for products or deliverables licensed to the State unless superseded by a Vendor's Warranties pursuant to Vendor's License or Support Agreements.

Purchasing State Agency or Agency shall mean the Agency purchasing the goods or Services.

Services shall mean the duties and tasks undertaken by the Vendor to fulfill the requirements and specifications of this solicitation.. Services include, without limitation, providing web browser access by authorized users to Vendor hosted Computer storage, databases, Support, documentation, and other functionalities, all as a Platform as a Service ("PaaS") .

State shall mean the State of North Carolina, the Department of Information Technology (DIT), or the Purchasing State Agency in its capacity as the Contracting Agency, as appropriate.

- 2) **STANDARDS:** Any Deliverables shall meet all applicable State and federal requirements, such as State or Federal Regulation, and NC State Chief Information Officer's (CIO) policy or regulation. Vendor will provide and maintain a quality assurance system or program that includes any Deliverables and will tender or provide to the State only those Deliverables that have been inspected and found to conform to the RFP specifications. All Deliverables are subject to operation, certification, testing and inspection, and any accessibility specifications.
- 3) **WARRANTIES:** Unless otherwise expressly provided, any goods Deliverables provided by the Vendor shall be warranted for a period of 90 days after acceptance.
- 4) **SUBCONTRACTING:** The Vendor may subcontract the performance of required Services with Resources under the Agreement only with the prior written consent of the State contracting authority. Vendor shall provide the State with complete copies of any agreements made by and between Vendor and all subcontractors. The selected Vendor remains solely responsible for the performance of its subcontractors. Subcontractors, if any, shall adhere to the same standards required of the selected Vendor and the Agreement. Any contracts made by the Vendor with a subcontractor shall include an affirmative statement that the State is an intended third party beneficiary of the Agreement; that the subcontractor has no agreement with the State; and that the State shall be indemnified by the Vendor for any claim presented by the subcontractor. Notwithstanding any other term herein, Vendor shall timely exercise its contractual remedies against any non-performing subcontractor and, when appropriate, substitute another subcontractor.
- 5) **TRAVEL EXPENSES:** All travel expenses should be included in the Vendor's proposed costs. Separately stated travel expenses will not be reimbursed. In the event that the Vendor, upon specific request in writing by the State, is deemed eligible to be reimbursed for travel expenses arising under the performance of the Agreement, reimbursement will be at the out-of-state rates set forth in N.C.G.S. §138-6; as amended from time to time. Vendor agrees to use the lowest available airfare not requiring a weekend stay and to use the lowest available rate for rental vehicles. All Vendor incurred travel expenses shall be billed on a monthly basis, shall be supported by receipt and shall be paid by the State within thirty (30) days after invoice approval. Travel expenses exceeding the foregoing rates shall not be paid by the State. The State will reimburse travel allowances only for days on which the Vendor is required to be in North Carolina performing Services under the Agreement.
- 6) **GOVERNMENTAL RESTRICTIONS:** In the event any restrictions are imposed by governmental requirements that necessitate alteration of the material, quality, workmanship, or performance of the Deliverables offered prior to delivery thereof, the Vendor shall provide written notification of the necessary alteration(s) to the Agency Contract Administrator. The State reserves the right to accept any such

alterations, including any price adjustments occasioned thereby, or to cancel the Agreement. The State may advise Vendor of any restrictions or changes in specifications required by North Carolina legislation, rule or regulatory authority that require compliance by the State. In such event, Vendor shall use its best efforts to comply with the required restrictions or changes. If compliance cannot be achieved by the date specified by the State, the State may terminate the Agreement and compensate Vendor for sums then due under the Agreement.

- 7) **PROHIBITION AGAINST CONTINGENT FEES AND GRATUITIES:** Vendor warrants that it has not paid, and agrees not to pay, any bonus, commission, fee, or gratuity to any employee or official of the State for the purpose of obtaining any Contract or award issued by the State. Vendor further warrants that no commission or other payment has been or will be received from or paid to any third party contingent on the award of any Contract by the State, except as shall have been expressly communicated to the State Purchasing Agent in writing prior to acceptance of the Agreement or award in question. Each individual signing below warrants that he or she is duly authorized by their respective Party to sign the Agreement and bind the Party to the terms and conditions of this RFP. Vendor and their authorized signatory further warrant that no officer or employee of the State has any direct or indirect financial or personal beneficial interest, in the subject matter of the Agreement; obligation or Contract for future award of compensation as an inducement or consideration for making the Agreement. Subsequent discovery by the State of non-compliance with these provisions shall constitute sufficient cause for immediate termination of all outstanding contracts. Violations of this provision may result in debarment of the Vendor(s) as permitted by 9 NCAC 06B..1206, or other provision of law.
- 8) **AVAILABILITY OF FUNDS:** Any and all payments to Vendor are expressly contingent upon and subject to the appropriation, allocation and availability of funds to the Agency for the purposes set forth in the Agreement. If the Agreement or any Purchase Order issued hereunder is funded in whole or in part by federal funds, the Agency's performance and payment shall be subject to and contingent upon the continuing availability of said federal funds for the purposes of the Agreement or Purchase Order. If the term of the Agreement extends into fiscal years subsequent to that in which it is approved, such continuation of the Agreement is expressly contingent upon the appropriation, allocation and availability of funds by the N.C. Legislature for the purposes set forth in this RFP. If funds to effect payment are not available, the Agency will provide written notification to Vendor. If the Agreement is terminated under this paragraph, Vendor agrees to take back any affected Deliverables and software not yet delivered under the Agreement, terminate any Services supplied to the Agency under the Agreement, and relieve the Agency of any further obligation thereof. The State shall remit payment for Deliverables and Services accepted prior to the date of the aforesaid notice in conformance with the payment terms.
- 9) **ACCEPTANCE PROCESS:**
- a) The State shall have the obligation to notify Vendor, in writing ten calendar days following provision, performance (under a provided milestone or otherwise as agreed) or delivery of any Services or other Deliverables described in the Agreement that are not acceptable.
 - b) Acceptance testing is required for all Vendor supplied software and software or platform services unless provided otherwise in the solicitation documents or a Statement of Work. The State may define such processes and procedures as may be necessary or proper, in its opinion and discretion, to ensure compliance with the State's specifications, and Vendor's Product Warranties and technical representations. The State shall have the obligation to notify Vendor, in writing and within thirty (30) days following installation of any software deliverable if it is not acceptable.
 - c) Acceptance of Services or other Deliverables including software or platform services may be controlled by an amendment hereto, or additional terms as agreed by the Parties consistent with IT Project management under GS §143B-1340.
 - d) The notice of non-acceptance shall specify in reasonable detail the reason(s) a Service or given Deliverable is unacceptable. Acceptance by the State shall not be unreasonably withheld; but may be conditioned or delayed as required for installation and/or testing of Deliverables. Final acceptance is expressly conditioned upon completion of any applicable inspection and testing procedures. Should a Service or Deliverable fail to meet any specifications or acceptance criteria, the State may exercise any and all rights hereunder. Services or Deliverables discovered to be defective or failing to conform

to the specifications may be rejected upon initial inspection or at any later time if the defects or errors contained in the Services or Deliverables or non-compliance with the specifications were not reasonably ascertainable upon initial inspection. If the Vendor fails to promptly cure or correct the defect or replace or re-perform the Services or Deliverables, the State reserves the right to cancel the Purchase Order, contract with a different Vendor, and to invoice the original Vendor for any differential in price over the original Contract price.

- 10) PAYMENT TERMS:** Monthly Payment terms are Net 30 days after receipt of correct invoice and acceptance of one or more of the Deliverables, under milestones or otherwise as may be provided in Paragraph 9 (Acceptance), or elsewhere in this solicitation, unless a period of more than thirty (30) days is required by the Agency. The Purchasing State Agency is responsible for all payments under the Agreement. No additional charges to the Agency will be permitted based upon, or arising from, the Agency's use of a Business Procurement Card. The State may exercise any and all rights of Set Off as permitted in Chapter 105A-1 *et. seq.* of the N.C. General Statutes and applicable Administrative Rules. Upon Vendor's written request of not less than thirty (30) days and approval by the State or Agency, the Agency may:
- a) Forward the Vendor's payment check(s) directly to any person or entity designated by the Vendor, or
 - b) Include any person or entity designated in writing by Vendor as a joint payee on the Vendor's payment check(s), however
 - c) In no event shall such approval and action obligate the State to anyone other than the Vendor and the Vendor shall remain responsible for fulfillment of all Contract obligations.
- 11) EQUAL EMPLOYMENT OPPORTUNITY:** Vendor shall comply with all Federal and State requirements concerning fair employment and employment of the disabled, and concerning the treatment of all employees without regard to discrimination by reason of race, color, religion, sex, national origin or physical disability.
- 12) ADVERTISING/PRESS RELEASE:** The Vendor absolutely shall not publicly disseminate any information concerning the Agreement without prior written approval from the State or its Agent. For the purpose of this provision of the Agreement, the Agent is the Purchasing Agency Contract Administrator unless otherwise named in the solicitation documents.
- 13) LATE DELIVERY:** Vendor shall advise the Agency contact person or office immediately upon determining that any Deliverable will not, or may not, be delivered or performed at the time or place specified. Together with such notice, Vendor shall state the projected delivery time and date. In the event the delay projected by Vendor is unsatisfactory, the Agency shall so advise Vendor and may proceed to procure the particular substitute Services or other Deliverables.
- 14) ACCESS TO PERSONS AND RECORDS:** Pursuant to N.C.G.S. §147-64.7, the Agency, the State Auditor, appropriate federal officials, and their respective authorized employees or agents are authorized to examine all books, records, and accounts of the Vendor insofar as they relate to transactions with any department, board, officer, commission, institution, or other agency of the State of North Carolina pursuant to the performance of the Agreement or to costs charged to the Agreement. The Vendor shall retain any such books, records, and accounts for a minimum of three (3) years after the completion of the Agreement. Additional audit or reporting requirements may be required by any Agency, if in the Agency's opinion, such requirement is imposed by federal or state law or regulation.
- 15) ASSIGNMENT:** Vendor may not assign the Agreement or its obligations hereunder except as permitted by 09 NCAC 06B.1003 and this Paragraph. Vendor shall provide reasonable notice of not less than thirty (30) days prior to any consolidation, acquisition, or merger. Any assignee shall affirm the Agreement attorning and agreeing to the terms and conditions agreed, and that Vendor shall affirm that the assignee is fully capable of performing all obligations of Vendor under the Agreement. An assignment may be made, if at all, in writing by the Vendor, Assignee and the State setting forth the foregoing obligation of Vendor and Assignee.
- 16) INSURANCE COVERAGE:** During the term of the Agreement, the Vendor at its sole cost and expense shall provide commercial insurance of such type and with such terms and limits as may be reasonably associated with the Agreement. As a minimum, the Vendor shall provide and maintain the following coverage and limits:

- a) **Worker's Compensation** - The Vendor shall provide and maintain Worker's Compensation Insurance, as required by the laws of North Carolina, as well as employer's liability coverage with minimum limits of \$100,000.00, covering all of Vendor's employees who are engaged in any work under the Agreement. If any work is sublet, the Vendor shall require the subcontractor to provide the same coverage for any of his employees engaged in any work under the Agreement; and
- b) **Commercial General Liability** - General Liability Coverage on a Comprehensive Broad Form on an occurrence basis in the minimum amount of \$2,000,000.00 Combined Single Limit (Defense cost shall be in excess of the limit of liability); and
- c) **Automobile** - Automobile Liability Insurance, to include liability coverage, covering all owned, hired and non-owned vehicles, used in connection with the Agreement. The minimum combined single limit shall be \$500,000.00 bodily injury and property damage; \$500,000.00 uninsured/under insured motorist; and \$5,000.00 medical payment; and
- d) Providing and maintaining adequate insurance coverage described herein is a material obligation of the Vendor and is of the essence of the Agreement. All such insurance shall meet all laws of the State of North Carolina. Such insurance coverage shall be obtained from companies that are authorized to provide such coverage and that are authorized by the Commissioner of Insurance to do business in North Carolina. The Vendor shall at all times comply with the terms of such insurance policies, and all requirements of the insurer under any such insurance policies, except as they may conflict with existing North Carolina laws or the Agreement. The limits of coverage under each insurance policy maintained by the Vendor shall not be interpreted as limiting the Vendor's liability and obligations under the Agreement.

17) DISPUTE RESOLUTION: The parties agree that it is in their mutual interest to resolve disputes informally. A claim by the Vendor shall be submitted in writing to the Agency Contract Administrator for decision. A claim by the State shall be submitted in writing to the Vendor's Contract Administrator for decision. The Parties shall negotiate in good faith and use all reasonable efforts to resolve such dispute(s). During the time the Parties are attempting to resolve any dispute, each shall proceed diligently to perform their respective duties and responsibilities under the Agreement. If a dispute cannot be resolved between the Parties within thirty (30) days after delivery of notice, either Party may elect to exercise any other remedies available under the Agreement, or at law. This term shall not constitute an agreement by either party to mediate or arbitrate any dispute.

18) CONFIDENTIALITY: In accordance with N.C.G.S. §143B-1350(e) and 143B-1375, and 09 NCAC 06B.0103 and 06B.1001, the State may maintain the confidentiality of certain types of information described in N.C.G.S. §132-1 *et seq.* Such information may include trade secrets defined by N.C.G.S. §66-152 and other information exempted from the Public Records Act pursuant to N.C.G.S. §132-1.2. Vendor may designate appropriate portions of its response as confidential, consistent with and to the extent permitted under the Statutes and Rules set forth above, by marking the top and bottom of pages containing confidential information with a legend in boldface type "**CONFIDENTIAL**". By so marking any page, the Vendor warrants that it has formed a good faith opinion, having received such necessary or proper review by counsel and other knowledgeable advisors that the portions marked confidential meet the requirements of the Rules and Statutes set forth above. ***However, under no circumstances shall price information be designated as confidential.*** The State may serve as custodian of Vendor's confidential information and not as an arbiter of claims against Vendor's assertion of confidentiality. If an action is brought pursuant to N.C.G.S. §132-9 to compel the State to disclose information marked confidential, the Vendor agrees that it will intervene in the action through its counsel and participate in defending the State, including any public official(s) or public employee(s). The Vendor agrees that it shall hold the State and any official(s) and individual(s) harmless from any and all damages, costs, and attorneys' fees awarded against the State in the action. The State agrees to promptly notify the Vendor in writing of any action seeking to compel the disclosure of Vendor's confidential information. The State shall have the right, at its option and expense, to participate in the defense of the action through its counsel. The State shall have no liability to Vendor with respect to the disclosure of Vendor's confidential information ordered by a court of competent jurisdiction pursuant to N.C.G.S. §132-9 or other applicable law.

- a) Care of Information: Vendor agrees to use commercial best efforts to safeguard and protect any data, documents, files, and other materials received from the State or the Agency during performance of any contractual obligation from loss, destruction or erasure. Vendor agrees to abide by all facilities and security requirements and policies of the agency where work is to be performed. Any Vendor personnel shall abide by such facilities and security requirements and shall agree to be bound by the terms and conditions of the Agreement.
- b) Vendor warrants that all its employees and any approved third party Vendors or subcontractors are subject to a non-disclosure and confidentiality agreement enforceable in North Carolina. Vendor will, upon request of the State, verify and produce true copies of any such agreements. Production of such agreements by Vendor may be made subject to applicable confidentiality, non-disclosure or privacy laws; provided that Vendor produces satisfactory evidence supporting exclusion of such agreements from disclosure under the N.C. Public Records laws in N.C.G.S. §132-1 *et seq.* The State may, in its sole discretion, provide a non-disclosure and confidentiality agreement satisfactory to the State for Vendor's execution. The State may exercise its rights under this subparagraph as necessary or proper, in its discretion, to comply with applicable security regulations or statutes including, but not limited to 26 USC 6103 and IRS Publication 1075, (Tax Information Security Guidelines for Federal, State, and Local Agencies), HIPAA, 42 USC 1320(d) (Health Insurance Portability and Accountability Act), any implementing regulations in the Code of Federal Regulations, and any future regulations imposed upon the Department of Information Technology or the N.C. Department of Revenue pursuant to future statutory or regulatory requirements.
- c) Nondisclosure: Vendor agrees and specifically warrants that it, its officers, directors, principals and employees, and any subcontractors, shall hold all information received during performance of the Agreement in the strictest confidence and shall not disclose the same to any third party without the express written approval of the State.
- d) The Vendor shall protect the confidentiality of all information, data, instruments, studies, reports, records and other materials provided to it by the Agency or maintained or created in accordance with this Agreement. No such information, data, instruments, studies, reports, records and other materials in the possession of Vendor shall be disclosed in any form without the prior written consent of the State Agency. The Vendor will have written policies governing access to and duplication and dissemination of all such information, data, instruments, studies, reports, records and other materials.
- e) All project materials, including software, data, and documentation created during the performance or provision of Services hereunder that are not licensed to the State or are not proprietary to the Vendor are the property of the State of North Carolina and must be kept confidential or returned to the State, or destroyed. Proprietary Vendor materials shall be identified to the State by Vendor prior to use or provision of Services hereunder and shall remain the property of the Vendor. Derivative works of any Vendor proprietary materials prepared or created during the performance of provision of Services hereunder shall be subject to a perpetual, royalty free, nonexclusive license to the State.

19) DEFAULT: In the event Services or other Deliverable furnished or performed by the Vendor during performance of any Contract term fail to conform to any material requirement(s) of the Contract specifications, notice of the failure is provided by the State and if the failure is not cured within ten (10) days, or Vendor fails to meet the requirements of Paragraph 9) herein, the State may cancel the contract. Default may be cause for debarment as provided in 09 NCAC 06B.1206. The rights and remedies of the State provided above shall not be exclusive and are in addition to any other rights and remedies provided by law or under the Contract.

- a) If Vendor fails to deliver or provide correct Services or other Deliverables within the time required by the Agreement, the State shall provide written notice of said failure to Vendor, and by such notice require performance assurance measures pursuant to N.C.G.S. 143B-1340(f). Vendor is responsible for the delays resulting from its failure to deliver or provide services or other Deliverables.
- b) Should the State fail to perform any of its obligations upon which Vendor's performance is conditioned, Vendor shall not be in default for any delay, cost increase or other consequences resulting from the State's failure. Vendor will use reasonable efforts to mitigate delays, costs or expenses arising from assumptions in the Vendor's offer documents that prove erroneous or are

otherwise invalid. Any deadline that is affected by any such failure in assumptions or performance by the State shall be extended by an amount of time reasonably necessary to compensate for the effect of such failure.

- c) Vendor shall provide a plan to cure any delay or default if requested by the State. The plan shall state the nature of the delay or default, the time required for cure, any mitigating factors causing or tending to cause the delay or default, and such other information as the Vendor may deem necessary or proper to provide.
- d) If the prescribed acceptance testing stated in the Solicitation Documents or performed pursuant to Paragraph 9) of the DIT Terms and Conditions is not completed successfully, the State may request substitute Software, cancel the portion of the Contract that relates to the unaccepted Software, or continue the acceptance testing with or without the assistance of Vendor. These options shall remain in effect until such time as the testing is successful or the expiration of any time specified for completion of the testing. If the testing is not completed after exercise of any of the State's options, the State may cancel any portion of the contract related to the failed Software and take action to procure substitute software. If the failed software (or the substituted software) is an integral and critical part of the proper completion of the work for which the Deliverables identified in the solicitation documents or statement of work were acquired, the State may terminate the entire contract.

20) WAIVER OF DEFAULT: Waiver by either party of any default or breach by the other Party shall not be deemed a waiver of any subsequent default or breach and shall not be construed to be a modification or novation of the terms of the Agreement, unless so stated in writing and signed by authorized representatives of the Agency and the Vendor, and made as an amendment to the Agreement pursuant to Paragraph 40) herein below.

21) TERMINATION: Any notice or termination made under the Agreement shall be transmitted via US Mail, Certified Return Receipt Requested. The period of notice for termination shall begin on the day the return receipt is signed and dated.

- a) The parties may mutually terminate the Agreement by written agreement at any time.
- b) The State may terminate the Agreement, in whole or in part, pursuant to Paragraph 19), or pursuant to the Special Terms and Conditions in the Solicitation Documents, if any, or for any of the following:
 - i) Termination for Cause: In the event any goods, software, or service furnished by the Vendor during performance of any Contract term fails to conform to any material requirement of the Contract, and the failure is not cured within the specified time after providing written notice thereof to Vendor, the State may cancel and procure the articles or Services from other sources; holding Vendor liable for any excess costs occasioned thereby, subject only to the limitations provided in Paragraphs 22) and 23) herein. The rights and remedies of the State provided above shall not be exclusive and are in addition to any other rights and remedies provided by law or under the Contract. Vendor shall not be relieved of liability to the State for damages sustained by the State arising from Vendor's breach of the Agreement; and the State may, in its discretion, withhold any payment due as a setoff until such time as the damages are finally determined or as agreed by the parties. Voluntary or involuntary Bankruptcy or receivership by Vendor shall be cause for termination.
 - ii) Termination For Convenience Without Cause: The State may terminate service and indefinite quantity contracts, in whole or in part by giving thirty (30) days prior notice in writing to the Vendor. Vendor shall be entitled to sums due as compensation for Deliverables provided and Services performed in conformance with the Contract. In the event the Contract is terminated for the convenience of the State the Agency will pay for all work performed and products delivered in conformance with the Contract up to the date of termination.
 - iii) Consistent failure to participate in problem resolution meetings, two (2) consecutive missed or rescheduled meetings, or failure to make a good faith effort to resolve problems, may result in termination of the Agreement.

22) LIMITATION OF VENDOR'S LIABILITY:

- a) Where Deliverables are under the State's exclusive management and control, the Vendor shall not be liable for direct damages caused by the State's failure to fulfill any State responsibilities of assuring the

proper use, management and supervision of the Deliverables and programs, audit controls, operating methods, office procedures, or for establishing all proper checkpoints necessary for the State's intended use of the Deliverables. Vendor shall not be responsible for any damages that arise from (i) misuse or modification of Vendor's Software by or on behalf of the State, (ii) the State's failure to use corrections or enhancements made available by Vendor, (iii) the quality or integrity of data from other automated or manual systems with which the Vendor's Software interfaces, (iv) errors in or changes to third party software or hardware implemented by the State or a third party (including the vendors of such software or hardware) that is not a subcontractor of Vendor or that is not supported by the Deliverables, or (vi) the operation or use of the Vendor's Software not in accordance with the operating procedures developed for the Vendor's Software or otherwise in a manner not contemplated by this Agreement.

- b) The Vendor's liability for damages to the State arising under the contract shall be limited to two times the value of the Contract.
- c) The foregoing limitation of liability shall not apply to claims covered by other specific provisions including but not limited to Service Level Agreement or Deliverable/Product Warranties pursuant to Section II, 2) of these Terms and Conditions, or to claims for injury to persons or damage to tangible personal property, gross negligence or willful or wanton conduct. This limitation of liability does not apply to contributions among joint tortfeasors under N.C.G.S. 1B-1 *et seq.*, the receipt of court costs or attorney's fees that might be awarded by a court in addition to damages after litigation based on the Agreement. For avoidance of doubt, the Parties agree that the Service Level Agreement and Deliverable/Product Warranty Terms in the Contract are intended to provide the sole and exclusive remedies available to the State under the Contract for the Vendor's failure to comply with the requirements stated therein.

23) VENDOR'S LIABILITY FOR INJURY TO PERSONS OR DAMAGE TO PROPERTY:

- a) The Vendor shall be liable for damages arising out of personal injuries and/or damage to real or tangible personal property of the State, employees of the State, persons designated by the State for training, or person(s) other than agents or employees of the Vendor, designated by the State for any purpose, prior to, during, or subsequent to delivery, installation, acceptance, and use of the Deliverables either at the Vendor's site or at the State's place of business, provided that the injury or damage was caused by the fault or negligence of the Vendor.
- b) The Vendor agrees to indemnify, defend and hold the Agency and the State and its Officers, employees, agents and assigns harmless from any liability relating to personal injury or injury to real or personal property of any kind, accruing or resulting to any other person, firm or corporation furnishing or supplying work, Services, materials or supplies in connection with the performance of the Agreement, whether tangible or intangible, arising out of the ordinary negligence, wilful or wanton negligence, or intentional acts of the Vendor, its officers, employees, agents, assigns or subcontractors.
- c) Vendor shall not be liable for damages arising out of or caused by an alteration or an attachment not made or installed by the Vendor.

24) TIME IS OF THE ESSENCE: Time is of the essence in the performance of the Agreement.

25) DATE AND TIME WARRANTY: The Vendor warrants that any Deliverable, whether Services, hardware, firmware, middleware, custom or commercial software, or internal components, subroutines, and interface therein which performs, modifies or affects any date and/or time data recognition function, calculation, or sequencing, will still enable the modified function to perform accurate date/time data and leap year calculations. This warranty shall survive termination or expiration of the Contract.

26) INDEPENDENT CONTRACTORS: Vendor and its employees, officers and executives, and subcontractors, if any, shall be independent Vendors and not employees or agents of the State. The Agreement shall not operate as a joint venture, partnership, trust, agency or any other similar business relationship.

27) TRANSPORTATION: Transportation of any tangible Deliverables shall be FOB Destination; unless otherwise specified in the solicitation document or purchase order. Freight, handling, hazardous material charges, and distribution and installation charges shall be included in the total price of each item. Any

additional charges shall not be honored for payment unless authorized in writing by the Purchasing State Agency. In cases where parties, other than the Vendor ship materials against this order, the shipper must be instructed to show the purchase order number on all packages and shipping manifests to ensure proper identification and payment of invoices. A complete packing list must accompany each shipment.

28) NOTICES: Any notices required under the Agreement should be delivered to the Contract Administrator for each party. Unless otherwise specified in the Solicitation Documents, any notices shall be delivered in writing by U.S. Mail, Commercial Courier or by hand.

29) TITLES AND HEADINGS: Titles and Headings in the Agreement are used for convenience only and do not define, limit or proscribe the language of terms identified by such Titles and Headings.

30) AMENDMENT: The Agreement may not be amended orally or by performance. Any amendment must be made in written form and signed by duly authorized representatives of the State and Vendor in conformance with Paragraph 36) herein.

31) TAXES: The State of North Carolina is exempt from Federal excise taxes and no payment will be made for any personal property taxes levied on the Vendor or for any taxes levied on employee wages. Agencies of the State may have additional exemptions or exclusions for federal or state taxes. Evidence of such additional exemptions or exclusions may be provided to Vendor by Agencies, as applicable, during the term of the Agreement. Applicable State or local sales taxes shall be invoiced as a separate item.

32) GOVERNING LAWS, JURISDICTION, AND VENUE:

a) The Agreement is made under and shall be governed and construed in accordance with the laws of the State of North Carolina and applicable Administrative Rules. The place of the Agreement or purchase order, its situs and forum, shall be Wake County, North Carolina, where all matters, whether sounding in Contract or in tort, relating to its validity, construction, interpretation and enforcement shall be determined. Vendor agrees and submits, solely for matters relating to the Agreement, to the jurisdiction of the courts of the State of North Carolina, and stipulates that Wake County shall be the proper venue for all matters.

b) Except to the extent the provisions of the Contract are clearly inconsistent therewith, the applicable provisions of the Uniform Commercial Code as modified and adopted in North Carolina shall govern the Agreement. To the extent the Contract entails both the supply of "goods" and "Services," such shall be deemed "goods" within the meaning of the Uniform Commercial Code, except when deeming such Services as "goods" would result in a clearly unreasonable interpretation.

33) FORCE MAJEURE: Neither party shall be deemed to be in default of its obligations hereunder if and so long as it is prevented from performing such obligations as a result of events beyond its reasonable control, including without limitation, fire, power failures, any act of war, hostile foreign action, nuclear explosion, riot, strikes or failures or refusals to perform under subcontracts, civil insurrection, earthquake, hurricane, tornado, or other catastrophic natural event or act of God.

34) COMPLIANCE WITH LAWS: The Vendor shall comply with all laws, ordinances, codes, rules, regulations, and licensing requirements that are applicable to the conduct of its business, including those of federal, state, and local agencies having jurisdiction and/or authority.

35) SEVERABILITY: In the event that a court of competent jurisdiction holds that a provision or requirement of the Agreement violates any applicable law, each such provision or requirement shall be enforced only to the extent it is not in violation of law or is not otherwise unenforceable and all other provisions and requirements of the Agreement shall remain in full force and effect. All promises, requirement, terms, conditions, provisions, representations, guarantees and warranties contained herein shall survive the expiration or termination date unless specifically provided otherwise herein, or unless superseded by applicable federal or State statute, including statutes of repose or limitation.

36) CHANGES: The Agreement and subsequent purchase order(s) is awarded subject to the provision of the specified Services and the shipment or provision of other Deliverables as specified herein. Any changes made to the Agreement or purchase order proposed by the Vendor are hereby rejected unless accepted in writing by the Agency or State Award Authority. The State shall not be responsible for Services or other Deliverables delivered without a purchase order from the Agency or State Award Authority.

37) FEDERAL INTELLECTUAL PROPERTY BANKRUPTCY PROTECTION ACT: The Parties agree that the Agency shall be entitled to all rights and benefits of the Federal Intellectual Property Bankruptcy Protection Act, Public Law 100-506, codified at 11 U.S.C. 365(n), and any amendments thereto.

38) ELECTRONIC PROCUREMENT (Applies to all contracts that include E-Procurement and are identified as such in the body of the solicitation document): Purchasing shall be conducted through the Statewide E-Procurement Services. The State's third party agent shall serve as the Supplier Manager for this E-Procurement Services. The Vendor shall register for the Statewide E-Procurement Services within two (2) business days of notification of award in order to receive an electronic purchase order resulting from award of the Agreement.

- a) **The successful Vendor(s) shall pay a transaction fee of 1.75% (.0175) on the total dollar amount (excluding sales taxes) of each purchase order issued through the Statewide E-Procurement Service.** This applies to all purchase orders, regardless of the quantity or dollar amount of the purchase order. The transaction fee shall neither be charged to nor paid by the State, or by any State approved users of the contract. The transaction fee shall not be stated or included as a separate item in the proposed contract or invoice. There are no additional fees or charges to the Vendor for the Services rendered by the Supplier Manager under the Agreement. Vendor will receive a credit for transaction fees they paid for the purchase of any item(s) if an item(s) is returned through no fault of the Vendor. Transaction fees are non-refundable when an item is rejected and returned, or declined, due to the Vendor's failure to perform or comply with specifications or requirements of the contract.
- b) Vendor, or its authorized Reseller, as applicable, will be invoiced monthly for the State's transaction fee by the Supplier Manager. The transaction fee shall be based on purchase orders issued for the prior month. Unless Supplier Manager receives written notice from the Vendor identifying with specificity any errors in an invoice within thirty (30) days of the receipt of invoice, such invoice shall be deemed to be correct and Vendor shall have waived its right to later dispute the accuracy and completeness of the invoice. Payment of the transaction fee by the Vendor is due to the account designated by the State within thirty (30) days after receipt of the correct invoice for the transaction fee, which includes payment of all portions of an invoice not in dispute. Within thirty (30) days of the receipt of invoice, Vendor may request in writing an extension of the invoice payment due date for that portion of the transaction fee invoice for which payment of the related goods by the governmental purchasing entity has not been received by the Vendor. If payment of the transaction fee invoice is not received by the State within this payment period, it shall be considered a material breach of contract. The Supplier Manager shall provide, whenever reasonably requested by the Vendor in writing (including electronic documents), supporting documentation from the E-Procurement Service that accounts for the amount of the invoice.
- c) The Supplier Manager will capture the order from the State approved user, including the shipping and payment information, and submit the order in accordance with the E-Procurement Services. Subsequently, the Supplier Manager will send those orders to the appropriate Vendor on State Contract. The State or State approved user, not the Supplier Manager, shall be responsible for the solicitation, offers received, evaluation of offers received, award of Contract, and the payment for goods delivered.
- d) Vendor agrees at all times to maintain the confidentiality of its user name and password for the Statewide E-Procurement Services. If a Vendor is a corporation, partnership or other legal entity, then the Vendor may authorize its employees to use its password. Vendor shall be responsible for all activity and all charges for such employees. Vendor agrees not to permit a third party to use the Statewide E-Procurement Services through its account. If there is a breach of security through the Vendor's account, Vendor shall immediately change its password and notify the Supplier Manager of the security breach by e-mail. Vendor shall cooperate with the state and the Supplier Manager to mitigate and correct any security breach.
- e) The transaction fee applies only to commodities obtained under this contract, if any. The transaction fee does not apply to services obtained under this contract.

39) PATENT, COPYRIGHT, AND TRADE SECRET PROTECTION:

- a) Vendor has created, acquired or otherwise has rights in, and may, in connection with the performance of Services for the State, employ, provide, create, acquire or otherwise obtain rights in various concepts, ideas, methods, methodologies, procedures, processes, know-how, techniques, models, templates and general purpose consulting and software tools, utilities and routines (collectively, the "Vendor technology"). To the extent that any Vendor technology is contained in any of the Services or Deliverables including any derivative works, the Vendor hereby grants the State a royalty-free, fully paid, worldwide, perpetual, non-exclusive license to use such Vendor technology in connection with the Services or Deliverables for the State's purposes.
- b) Vendor shall not acquire any right, title and interest in and to the copyrights for goods, any and all software, technical information, specifications, drawings, records, documentation, data or derivative works thereof, or other work products provided by the State to Vendor. The State hereby grants Vendor a royalty-free, fully paid, worldwide, perpetual, non-exclusive license for Vendor's internal use to non-confidential deliverables first originated and prepared by the Vendor for delivery to the State.
- c) The Vendor, at its own expense, shall defend any action brought against the State to the extent that such action is based upon a claim that the Services or other Deliverables supplied by the Vendor, or the operation of such pursuant to a current version of vendor-supplied software, infringes a patent, or copyright or violates a trade secret in the United States. The Vendor shall pay those costs and damages finally awarded against the State in any such action; damages shall be limited as provided in N.C.G.S. 143B-1350(h1). Such defense and payment shall be conditioned on the following:
 - i. That the Vendor shall be notified within a reasonable time in writing by the State of any such claim; and,
 - ii. That the Vendor shall have the sole control of the defense of any action on such claim and all negotiations for its settlement or compromise, provided, however, that the State shall have the option to participate in such action at its own expense.
- d) Should any Services or other Deliverables supplied by Vendor, or the operation thereof become, or in the Vendor's opinion are likely to become, the subject of a claim of infringement of a patent, copyright, or a trade secret in the United States, the State shall permit the Vendor, at its option and expense, either to procure for the State the right to continue using the Services or Deliverables, or to replace or modify the same to become noninfringing and continue to meet procurement specifications in all material respects. If neither of these options can reasonably be taken, or if the use of such Services or Deliverables by the State shall be prevented by injunction, the Vendor agrees to take back any goods/hardware or software, and refund any sums the State has paid Vendor less any reasonable amount for use or damage and make every reasonable effort to assist the state in procuring substitute Services or Deliverables. If, in the sole opinion of the State, the return of such infringing Services or Deliverables makes the retention of other Services or Deliverables acquired from the Vendor under the agreement impractical, the State shall then have the option of terminating the contract, or applicable portions thereof, without penalty or termination charge. The Vendor agrees to take back Services or Deliverables and refund any sums the State has paid Vendor less any reasonable amount for use or damage.
- e) Vendor will not be required to defend or indemnify the State if any claim by a third party against the State for infringement or misappropriation (i) results from the State's alteration of any Vendor-branded Service or Deliverable, or (ii) results from the continued use of the good(s) or services and other Services or Deliverables after receiving notice they infringe a trade secret of a third party.
- f) Nothing stated herein, however, shall affect Vendor's ownership in or rights to its preexisting intellectual property and proprietary rights.

40) UNANTICIPATED TASKS In the event that additional work must be performed that was wholly unanticipated, and that is not specified in the Agreement, but which in the opinion of both parties is necessary to the successful accomplishment of the contracted scope of work, the procedures outlined in this article will be followed. For each item of unanticipated work, the Vendor shall prepare a work authorization in accordance with the State's practices and procedures.

- a) It is understood and agreed by both parties that all of the terms and conditions of the Agreement shall remain in force with the inclusion of any work authorization. A work authorization shall not constitute a contract separate from the Agreement, nor in any manner amend or supersede any of the other terms or provisions of the Agreement or any amendment hereto.
- b) Each work authorization shall comprise a detailed statement of the purpose, objective, or goals to be undertaken by the Vendor, the job classification or approximate skill level or sets of the personnel required, an identification of all significant material then known to be developed by the Vendor's personnel as a Deliverable, an identification of all significant materials to be delivered by the State to the Vendor's personnel, an estimated time schedule for the provision of the Services by the Vendor, completion criteria for the work to be performed, the name or identification of Vendor's personnel to be assigned, the Vendor's estimated work hours required to accomplish the purpose, objective or goals, the Vendor's billing rates and units billed, and the Vendor's total estimated cost of the work authorization.
- c) All work authorizations must be submitted for review and approval by the procurement office that approved the original Contract and procurement. This submission and approval must be completed prior to execution of any work authorization documentation or performance thereunder. All work authorizations must be written and signed by the Vendor and the State prior to beginning work.
- d) The State has the right to require the Vendor to stop or suspend performance under the "Stop Work" provision of the North Carolina Department of Information Technology Terms and Conditions.
- e) The Vendor shall not expend Personnel resources at any cost to the State in excess of the estimated work hours unless this procedure is followed: If, during performance of the work, the Vendor determines that a work authorization to be performed under the Agreement cannot be accomplished within the estimated work hours, the Vendor will be required to complete the work authorization in full. Upon receipt of such notification, the State may:
 - a. Authorize the Vendor to expend the estimated additional work hours or service in excess of the original estimate necessary to accomplish the work authorization, or
 - b. Terminate the work authorization, or
 - c. Alter the scope of the work authorization in order to define tasks that can be accomplished within the remaining estimated work hours.
 - d. The State will notify the Vendor in writing of its election within seven (7) calendar days after receipt of the Vendor's notification. If notice of the election is given to proceed, the Vendor may expend the estimated additional work hours or Services.

41) STOP WORK ORDER The State may issue a written Stop Work Order to Vendor for cause at any time requiring Vendor to suspend or stop all, or any part, of the performance due under the Agreement for a period up to ninety (90) days after the Stop Work Order is delivered to the Vendor. The ninety (90) day period may be extended for any further period for which the parties may agree.

- a) The Stop Work Order shall be specifically identified as such and shall indicate that it is issued under this term. Upon receipt of the Stop Work Order, the Vendor shall immediately comply with its terms and take all reasonable steps to minimize incurring costs allocable to the work covered by the Stop Work Order during the period of work suspension or stoppage. Within a period of ninety (90) days after a Stop Work Order is delivered to Vendor, or within any extension of that period to which the parties agree, the State shall either:
 - i) Cancel the Stop Work Order, or
 - ii) Terminate the work covered by the Stop Work Order as provided for in the termination for default or the termination for convenience clause of the Agreement.

- b) If a Stop Work Order issued under this clause is canceled or the period of the Stop Work Order or any extension thereof expires, the Vendor shall resume work. The State shall make an equitable adjustment in the delivery schedule, the Agreement price, or both, and the Agreement shall be modified, in writing, accordingly, if:
 - i) The Stop Work Order results in an increase in the time required for, or in the Vendor's cost properly allocable to the performance of any part of the Agreement, and
 - ii) The Vendor asserts its right to an equitable adjustment within thirty (30) days after the end of the period of work stoppage; provided that if the State decides the facts justify the action, the State may receive and act upon an offer submitted at any time before final payment under the Agreement.
- c) If a Stop Work Order is not canceled and the work covered by the Stop Work Order is terminated in accordance with the provision entitled Termination for Convenience of the State, the State shall allow reasonable direct costs resulting from the Stop Work Order in arriving at the termination settlement.
- d) The State shall not be liable to the Vendor for loss of profits because of a Stop Work Order issued under this term.

41) TRANSITION ASSISTANCE If the Agreement is not renewed at the end of the term, or is canceled prior to its expiration, for any reason, the Vendor must provide for up to six (6) months after the expiration or cancellation of the Agreement, all reasonable transition assistance requested by the State, to allow for the expired or canceled portion of the Services to continue without interruption or adverse effect, and to facilitate the orderly transfer of such Services to the State or its designees. Such transition assistance will be deemed by the parties to be governed by the terms and conditions of the Agreement, (notwithstanding this expiration or cancellation) except for those Contract terms or conditions that do not reasonably apply to such transition assistance. The State shall pay the Vendor for any resources utilized in performing such transition assistance at the most current rates provided by the Agreement for Contract performance. If the State cancels the Agreement for cause, then the State will be entitled to off set the cost of paying the Vendor for the additional resources the Vendor utilized in providing transition assistance with any damages the State may have otherwise accrued as a result of said cancellation.

42) STATE PROPERTY AND INTANGIBLES RIGHTS: The parties acknowledge and agree that the State shall own all right, title and interest in and to the copyright in any and all software, technical information, specifications, drawings, records, documentation, data and other work products first originated and prepared by the Vendor for delivery to the State (the "Deliverables"). To the extent that any Vendor Technology is contained in any of the Deliverables, the Vendor hereby grants the State a royalty-free, fully paid, worldwide, perpetual, non-exclusive license to use such Vendor Technology in connection with the Deliverables for the State's internal business purposes. Vendor shall not acquire any right, title and interest in and to the copyrights for goods, any and all software, technical information, specifications, drawings, records, documentation, data or derivative works thereof, or other work products provided by the State to Vendor. The State hereby grants Vendor a royalty-free, fully paid, worldwide, perpetual, non-exclusive license to non-confidential Deliverables first originated and prepared by the Vendor for delivery to the State.

Section 2: Terms and Conditions Applicable to Vendor Hosted Services (e.g., Platform as a Service ("PaaS"); Infrastructure as a Service ("IaaS"))

1) DEFINITIONS:

- a) "Data" includes all materials provided by the State to the Vendor, including but not limited to software, technical information, specifications, drawings, records, and documentation, as well as includes and means the information, formulae, algorithms, or other content that the State, the State's employees, agents and end users upload, create or modify using the Services pursuant to this Agreement. Data

also includes user identification information and metadata which may contain Data or from which the State's Data may be ascertainable.

- b) "Support" includes provision of ongoing updates and maintenance for the Vendor online software applications, and as may be specified herein, consulting, training and other support Services as provided by the Vendor to meet the requirements and specifications of this RFP and for Vendor's tenants receiving similar Services.

2) **ACCESS AND USE OF VENDOR HOSTED SERVICES:**

- a) The Vendor grants the State a personal non-transferable and non-exclusive right to use and access, all Services and other functionalities or services provided, furnished or accessible under this Agreement. The State is authorized to access the State's Data and any Vendor-provided data as specified herein and to transmit revisions, updates, deletions, enhancements, or modifications to the State Data. The State may use the Services with any computer, computer system, server, or desktop workstation owned or utilized by the State or other authorized users. User access to the Services shall be routinely provided by the Vendor. All Services and information designated by Vendor as "confidential" or "proprietary" shall be kept in confidence except as may be required by the North Carolina Public Records Act: N.C.G.S. § 132-1, *et. seq.*
- b) The State's access license for the Services and its associated services neither transfers, vests, nor infers any title or other ownership right in any intellectual property rights of the Vendor or any third party, nor does this license transfer, vest, or infer any title or other ownership right in any Vendor source code associated with the Services unless otherwise agreed to by the parties. The provisions of this paragraph will not be construed as a sale of any ownership rights in the Services. Any Services or technical and business information owned by Vendor or its suppliers or licensors made accessible or furnished to the State shall be and remain the property of the Vendor or such other party, respectively. Vendor has a limited, non-exclusive license to access and use the State Data as provided to Vendor, but solely for performing its obligations under this Agreement and in confidence as provided herein.
- c) The Vendor or its suppliers shall at minimum, and except as otherwise agreed, provide telephone assistance to the State for all Services procured hereunder during the State's normal business hours (unless different hours are specified herein). The Vendor warrants that its Support and customer service and assistance will be performed in accordance with generally accepted industry standards. The State has the right to receive the benefit of upgrades, updates, maintenance releases or other enhancements or modifications made generally available to the Vendor's tenants for similar Services.
- d) The Vendor will provide to the State Services for updating, maintaining and continuing optimal performance for the Services. Unless otherwise agreed in writing, Support will also be provided for any other (e.g., third party) software provided by the Vendor in connection with the Vendor's solution herein. The technical and professional activities required for establishing, managing, and maintaining the Services environment are the responsibilities of the Vendor. Any training specified herein will be provided by the Vendor to certain State users for the fees or costs as set forth herein or in an SLA.
- e) Services provided pursuant to this Solicitation may, in some circumstances, be accompanied by a user clickwrap agreement. The term clickwrap agreement refers to an agreement that requires the end user to manifest his or her assent to terms and conditions by clicking an "ok" or "agree" button on a dialog box or pop-up window as part of the process of access to the Services. All terms and conditions of any clickwrap agreement provided with any Services solicited herein shall have no force and effect and shall be non-binding on the State, its employees, agents, and other authorized users of the Services.
- f) The Vendor may utilize partners and/or subcontractors to assist in the provision of the Services, so long as the State Data is not removed from the United States unless the terms of storage of the State Data are clearly disclosed, the security provisions referenced herein can still be complied with, and such removal is done with the prior express written permission of the State. The Vendor shall identify all of its strategic business partners related to Services provided under this contract including, but not limited to, all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Vendor, who will be involved in any application development and/or operations.
- g) The Vendor warrants that all Services will be performed with professional care and skill, in a workmanlike manner and in accordance with the Services documentation and this Agreement.

- h) Reserved..
 - i) Professional services provided by the Vendor at the request by the State in writing in addition to agreed Services shall be at the then-existing Vendor hourly rates when provided, unless otherwise agreed in writing by the parties.
- 3) **WARRANTY OF NON-INFRINGEMENT:**
- a) The Vendor warrants to the best of its knowledge that:
 - i) The Services do not infringe any intellectual property rights of any third party; and
 - ii) There are no actual or threatened actions arising from, or alleged under, any intellectual property rights of any third party.
- 4) **ACCESS AVAILABILITY; REMEDIES:**
- a) The Vendor warrants that the Services will be in good working order, and operating in conformance with Vendor's standard specifications and functions as well as any other specifications agreed to by the parties in writing, and shall remain accessible 24/7, with the exception of scheduled outages for maintenance and of other service level provisions agreed in writing, e.g., in an SLA..
 - b) The State shall notify the Vendor if the Services are not in good working order or inaccessible during the term of the Agreement. The Vendor shall, at its option, either repair, replace or reperform any Services reported or discovered as not being in good working order and accessible during the applicable contract term without cost to the State.
 - c) Support Services. Reserved..
- 5) **EXCLUSIONS:**
- a) Except as stated above in Paragraphs 3 and 4, Vendor and its parent, subsidiaries and affiliates, subcontractors and suppliers make no warranties, express or implied, as to the Services.
 - b) The warranties provided in Paragraphs 3 and 4 above do not cover repair for damages, malfunctions or service failures substantially caused by:
 - i) Actions of non-Vendor personnel;
 - ii) Failure to follow Vendor's written instructions relating to the Services provided to the State; or
 - iii) Force Majeure conditions set forth hereinbelow.
 - iv) The State's sole misuse of, or its own inability to use, the Services.
- 6) **PERFORMANCE REVIEW AND ACCOUNTABILITY:** N.C.G.S. § 143B-1340(f) and 09 NCAC 06B.1207 require provisions for performance review and accountability in State IT contracts. For this procurement, these shall include the holding a retainage of ten percent (10%) of each applicable monthly Maintenance and Enhancement value in Attachment D, plus 10% of each applicable monthly Hosting value in Attachment D, and withholding the final payment contingent on final acceptance by the State as provided in 09 NCAC 06B.1207(3) and (4), unless waived or otherwise agreed, in writing. The Services herein will be provided consistent with and under these Services performance review and accountability guarantees.
- 7) **LIMITATION OF LIABILITY: Limitation of Vendor's Contract Damages Liability:** Reserved.
- 8) **VENDOR'S LIABILITY FOR INJURY TO PERSONS OR DAMAGE TO PROPERTY:** Reserved.
- 9) **MODIFICATION OF SERVICES:** Reserved..
- 10) **TRANSITION PERIOD:**
- a) For up to six (6) months, either prior to the expiration date of this Agreement, or upon notice of termination of this Agreement, the Vendor shall assist the State, upon written request, in extracting and/or transitioning all Data, source code, and all other work products in the format determined by the State ("Transition Period").
 - b) The Transition Period may be modified in an SLA or as agreed upon in writing by the parties in a contract amendment.
 - c) During the Transition Period, Services access shall continue to be made available to the State without alteration.
 - d) The Vendor agrees to compensate the State for damages or losses the State incurs as a result of Vendor's failure to comply with this Transition Period section in accordance with the Limitation of Liability provisions above.
 - e) Upon termination, and unless otherwise stated in an SLA, and after providing the State Data to the State as indicated above in this section with acknowledged receipt by the State in writing, the Vendor shall

permanently destroy or render inaccessible any portion of the State Data in the Vendor's and/or subcontractor's possession or control following the completion and expiration of all obligations in this section. Within thirty (30) days, the Vendor shall issue a written statement to the State confirming the destruction or inaccessibility of the State's Data.

- f) The State at its option, may purchase additional Transition Services as may be agreed upon in a supplemental agreement.

11) **TRANSPORTATION:** Transportation charges for any Deliverable sent to the State other than electronically or by download shall be FOB Destination unless delivered by internet or file-transfer as agreed by the State, or otherwise specified in the solicitation document or purchase order.

12) **PAYMENT TERMS (Applicable to SaaS): Reserved.**

13) **SECURITY OF STATE DATA**

- a) All Data provided by the State to the Vendor (State Data) during the performance or provision of Services hereunder are the property of the State of North Carolina and must be kept secure and returned to the State. The Vendor will protect State Data in its hands from unauthorized disclosure, loss, damage, destruction by natural event, or other eventuality. Proprietary Vendor materials shall be identified to the State by the Vendor prior to use or provision of Services hereunder and shall remain the property of the Vendor. Derivative works of any Vendor proprietary materials prepared or created during the performance of provision of Services hereunder shall be provided to the State as part of the Services. The Vendor shall not access State User accounts, or State Data, except (i) during data center operations; (ii) in response to service or technical issues; (iii) as required by the express terms of this contract; or (iv) at the State's written request. The Vendor shall protect the confidentiality of all information, Data, instruments, studies, reports, records and other materials provided to it by the State or maintained or created in accordance with this Agreement. No such information, Data, instruments, studies, reports, records and other materials in the possession of Vendor shall be disclosed in any form without the prior written agreement with the State. The Vendor will have written policies governing access to and duplication and dissemination of all such information, Data, instruments, studies, reports, records and other materials.
- b) The Vendor shall not store or transfer non-public State data outside of the United States. This includes backup data and Disaster Recovery locations. The Service Provider will permit its personnel and contractors to access State of North Carolina data remotely only as required to provide technical support.
- c) Protection of personal privacy and sensitive data. The Vendor acknowledges its responsibility for securing any restricted or highly restricted data, as defined by the Statewide Data Classification and Handling Policy (<https://it.nc.gov/document/statewide-data-classification-and-handling-policy>) that is collected by the State and stored in any Vendor site or other Vendor housing systems including, but not limited to, computer systems, networks, servers, or databases, maintained by Vendor or its agents or subcontractors in connection with the provision of the Services. The Vendor warrants, at its sole cost and expense, that it shall implement processes and maintain the security of data classified as restricted or highly restricted; provide reasonable care and efforts to detect fraudulent activity involving the data; and promptly notify the State of any breaches of security within twenty-four (24) hours of confirmation as required by N.C.G.S. § 143B-1379.
- d) The Vendor will provide and maintain secure backup of the State Data. The Vendor shall implement and maintain secure passwords for its online system providing the Services, as well as all appropriate administrative, physical, technical and procedural safeguards at all times during the term of this Agreement to secure such Data from Data Breach, protect the Data and the Services from loss, corruption, unauthorized disclosure, and the introduction of viruses, disabling devices, malware and other forms of malicious or inadvertent acts that can disrupt the State's access to its Data and the Services. The Vendor will allow periodic back-up of State Data by the State to the State's infrastructure as the State requires or as may be provided by law.
- e) The Vendor shall certify to the State:
 - i) The sufficiency of its security standards, tools, technologies and procedures in providing Services under this Agreement;

- ii) That the system used to provide the Subscription Services under this Contract has and will maintain a valid third party security certification not to exceed one (1) year and is consistent with the data classification level and a security controls appropriate for low or moderate information system(s) per the National Institute of Standards and Technology NIST 800-53 revision 4. The State reserves the right to independently evaluate, audit, and verify such requirements.
- iii) That the Services will comply with the following:
 - (1) Any DIT security policy regarding Cloud Computing, and the DIT Statewide Information Security Policy Manual; to include encryption requirements as defined below:
 - (a) The Vendor shall encrypt all non-public data in transit regardless of the transit mechanism.
 - (b) For engagements where the Vendor stores sensitive personally identifiable or otherwise confidential information, this data shall be encrypted at rest. Examples are social security number, date of birth, driver's license number, financial data, federal/state tax information, and hashed passwords. The Vendor's encryption shall be consistent with validated cryptography standards as specified in National Institute of Standards and Technology FIPS140-2, Security Requirements. The key location and other key management details will be discussed and negotiated by both parties. When the Service Provider cannot offer encryption at rest, it must maintain, for the duration of the contract, cyber security liability insurance coverage for any loss resulting from a data breach. Additionally, where encryption of data at rest is not possible, the Vendor must describe existing security measures that provide a similar level of protection;
 - (2) Privacy provisions of the Federal Privacy Act of 1974;
 - (3) The North Carolina Identity Theft Protection Act, N.C.G.S. Chapter 75, Article 2A (e.g., N.C.G.S. § 75-65 and -66);
 - (4) The North Carolina Public Records Act, N.C.G.S. Chapter 132;
 - (5) Applicable Federal, State and industry standards and guidelines including, but not limited to, relevant security provisions of the Payment Card Industry (PCI) Data Security Standard (PCIDSS) including the PCIDSS Cloud Computing Guidelines, Criminal Justice Information, The Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA); and
 - (6) Any requirements implemented by the State under N.C.G.S. §§ 143B-1376 and -1377.
 - (7) Any requirements implemented by the State under N.C.G.S. §§ 20-309.2(d).
- f) Security Breach. "Security Breach" under the NC Identity Theft Protection Act (N.C.G.S. § 75-60 *et seq.*) means (1) any circumstance pursuant to which applicable Law requires notification of such breach to be given to affected parties or other activity in response to such circumstance (e.g., N.C.G.S. § 75-65); or (2) any actual, attempted, suspected, threatened, or reasonably foreseeable circumstance that compromises, or could reasonably be expected to compromise, either Physical Security or Systems Security (as such terms are defined below) in a fashion that either does or could reasonably be expected to permit unauthorized Processing (as defined below), use, disclosure or acquisition of or access to any the State Data or state confidential information. "Physical Security" means physical security at any site or other location housing systems maintained by Vendor or its agents or subcontractors in connection with the Services. "Systems Security" means security of computer, electronic or telecommunications systems of any variety (including data bases, hardware, software, storage, switching and interconnection devices and mechanisms), and networks of which such systems are a part or communicate with, used directly or indirectly by Vendor or its agents or subcontractors in connection with the Services. "Processing" means any operation or set of operations performed upon the State Data or State confidential information, whether by automatic means, such as creating, collecting, procuring, obtaining, accessing, recording, organizing, storing, adapting, altering, retrieving, consulting, using, disclosing or destroying.
- g) Breach Notification. In the event the Vendor becomes aware of any Security Breach due to Vendor acts or omissions other than in accordance with the terms of the Agreement, the Vendor shall, at its own expense, (1) immediately notify the State's Agreement Administrator of such Security Breach and perform a root cause analysis thereon; (2) investigate such Security Breach; (3) provide a remediation plan,

acceptable to the State, to address the Security Breach and prevent any further incidents; (4) conduct a forensic investigation to determine what systems, data and information have been affected by such event; and (5) cooperate with the State, and any law enforcement or regulatory officials, credit reporting companies, and credit card associations investigating such Security Breach. The State shall make the final decision on notifying the State's persons, entities, employees, service providers and/or the public of such Security Breach, and the implementation of the remediation plan. If a notification to a customer is required under any Law or pursuant to any of the State's privacy or security policies, then notifications to all persons and entities who are affected by the same event (as reasonably determined by the State) shall be considered legally required.

- h) Notification Related Costs. The Vendor shall issue notifications and shall pay all Notification Related Costs arising out of or in connection with any such Security Breach due to Vendor acts or omissions other than in accordance with the terms of the Agreement resulting in a requirement for legally required notifications. "Notification Related Costs" shall include costs associated with addressing and responding to the Security Breach including, but not limited to, (1) preparation and mailing or other transmission of legally required notifications; (2) preparation and mailing or other transmission of such other communications to customers, agents or others as the State deems reasonably appropriate; (3) establishment of a call center or other communications procedures in response to such Security Breach (e.g., customer service FAQs, talking points and training); (4) public relations and other similar crisis management services; (5) legal and accounting fees and expenses associated with the State's investigation of and response to such event; and (6) costs for credit reporting services that are associated with legally required notifications or are advisable, in the State's opinion, under the circumstances. If the Vendor becomes aware of any Security Breach which is not due to Vendor acts or omissions other than in accordance with the terms of the Agreement, the Vendor shall immediately notify the State of such Security Breach, and the parties shall reasonably cooperate regarding which of the foregoing or other activities may be appropriate under the circumstances, including any applicable Charges for the same.
- i) The Vendor shall allow the State reasonable access to Services security logs, latency statistics, and other related Services security data that affect this Agreement and the State's Data, at no cost to the State.
- j) In the course of normal operations, it may become necessary for the Vendor to copy or move Data to another storage destination on its online system, and delete the Data found in the original location. In any such event, the Vendor shall preserve and maintain the content and integrity of the Data, except by prior written notice to, and prior written approval by, the State.
- k) Remote access to Data from outside the continental United States including, without limitation, remote access to Data by authorized Services support staff in identified support centers, is prohibited unless approved in advance by the State Chief Information Officer or the Using Agency.
- l) In the event of temporary loss of access to Services, the Vendor shall promptly restore continuity of Services, restore Data in accordance with this Agreement and as may be set forth in an SLA, restore accessibility of Data and the Services to meet the performance requirements stated herein or in an SLA. As a result, Service Level remedies will become available to the State as provided herein, in the SLA or other agreed and relevant documents. Failure to promptly remedy any such temporary loss of access may result in the State exercising its options for assessing damages under this Agreement.
- m) In the event of disaster or catastrophic failure that results in significant State Data loss or extended loss of access to Data or Services, the Vendor shall notify the State by the fastest means available and in writing, with additional notification provided to the State Chief Information Officer or designee of the contracting agency. Vendor shall provide such notification within twenty-four (24) hours after Vendor reasonably believes there has been such a disaster or catastrophic failure. In the notification, Vendor shall inform the State of:
 - (1) The scale and quantity of the State Data loss;
 - (2) What Vendor has done or will do to recover the State Data from backups and mitigate any deleterious effect of the State Data and Services loss; and
 - (3) What corrective action Vendor has taken or will take to prevent future State Data and Services loss.
 - (4) If Vendor fails to respond immediately and remedy the failure, the State may exercise its options for assessing damages or other remedies under this Agreement.

The Vendor shall investigate the disaster or catastrophic failure and shall share the report of the investigation with the State. The State and/or its authorized agents shall have the right to lead (if required by law) or participate in the investigation. The Vendor shall cooperate fully with the State, its agents and law enforcement.

- n) In the event of termination of this contract, cessation of business by the Vendor or other event preventing the Vendor from continuing to provide the Services, the Vendor shall not withhold the State Data or any other State confidential information or refuse, for any reason, to promptly return to the State the State Data and any other State confidential information (including copies thereof) if requested to do so on such media as reasonably requested by the State, even if the State is then or is alleged to be in breach of the Agreement. As a part of the Vendor's obligation to provide the State Data pursuant to this Paragraph 18) n), the Vendor will also provide the State any data maps, documentation, software, or other materials necessary, including, without limitation, handwritten notes, materials, working papers or documentation, for the State to use, translate, interpret, extract and convert the State Data.
- o) Secure Data Disposal. When requested by the State, the Vendor shall destroy all requested data in all of its forms (e.g., disk, CD/DVD, backup tape, and paper). Data shall be permanently deleted and shall not be recoverable, in accordance with National Institute of Standards and Technology (NIST) approved methods, and certificates of destruction shall be provided to the State.

Section 3: Terms and Conditions Applicable to Personnel and Personal Services

- 1) **VENDOR'S REPRESENTATION:** Vendor warrants that qualified personnel will provide Services in a professional manner. "Professional manner" means that the personnel performing the Services will possess the skill and competence consistent with the prevailing business standards in the information technology industry. Vendor agrees that it will not enter any agreement with a third party that might abridge any rights of the State under the Agreement. Vendor will serve as the prime Vendor under the Agreement. Should the State approve any subcontractor(s), the Vendor shall be legally responsible for the performance and payment of the subcontractor(s). Names of any third party Vendors or subcontractors of Vendor may appear for purposes of convenience in Contract documents; and shall not limit Vendor's obligations hereunder. Such third party subcontractors, if approved, may serve as subcontractors to Vendor. Vendor will retain executive representation for functional and technical expertise as needed in order to incorporate any work by third party subcontractor(s).
 - a) Intellectual Property. Vendor represents that it has the right to provide the Services and other Deliverables without violating or infringing any law, rule, regulation, copyright, patent, trade secret or other proprietary right of any third party. Vendor also represents that its Services and other Deliverables are not the subject of any actual or threatened actions arising from, or alleged under, any intellectual property rights of any third party.
 - b) Inherent Services. If any Services or other Deliverables, functions, or responsibilities not specifically described in the Agreement are required for Vendor's proper performance, provision and delivery of the Services and other Deliverables pursuant to the Agreement, or are an inherent part of or necessary sub-task included within the Services, they will be deemed to be implied by and included within the scope of the Contract to the same extent and in the same manner as if specifically described in the Contract.
 - c) Vendor warrants that it has the financial capacity to perform and to continue to perform its obligations under the Contract; that Vendor has no constructive or actual knowledge of an actual or potential legal proceeding being brought against Vendor that could materially adversely affect performance of the Agreement; and that entering into the Agreement is not prohibited by any Contract, or order by any court of competent jurisdiction.
- 2) **SERVICES PROVIDED BY VENDOR:** Vendor shall provide the State with implementation Services as specified in a Statement of Work ("SOW") executed by the parties. This Agreement in combination with each SOW individually comprises a separate and independent contractual obligation from any other SOW. A breach by Vendor under one SOW will not be considered a breach under any other SOW. The Services intended hereunder are related to the State's implementation and/or use of one or more

Software Deliverables licensed hereunder or in a separate software license agreement between the parties ("License Agreement"). (Reserve if not needed)

- 3) **PERSONNEL**: Vendor shall not substitute key personnel assigned to the performance of the Agreement without prior written approval by the Agency Contract Administrator. The individuals designated as key personnel for purposes of the Agreement are those specified in the Vendor's offer. Any desired substitution shall be noticed to the Agency's Contract Administrator in writing accompanied by the names and references of Vendor's recommended substitute personnel. The Agency will approve or disapprove the requested substitution in a timely manner. The Agency may, in its sole discretion, terminate the Services of any person providing Services under the Agreement. Upon such termination, the Agency may request acceptable substitute personnel or terminate the Contract Services provided by such personnel.
- a) Unless otherwise expressly provided in the Contract, Vendor will furnish all of its own necessary management, supervision, labor, facilities, furniture, computer and telecommunications equipment, software, supplies and materials necessary for the Vendor to provide and deliver the Services and other Deliverables.
 - b) Vendor personnel shall perform their duties on the premises of the State, during the State's regular work days and normal work hours, except as may be specifically agreed otherwise, established in the specification, or statement of work.
 - c) The Agreement shall not prevent Vendor or any of its personnel supplied under the Agreement from performing similar Services elsewhere or restrict Vendor from using the personnel provided to the State, provided that:
 - i) Such use does not conflict with the terms, specifications or any amendments to the Agreement, or
 - ii) Such use does not conflict with any procurement law, regulation or policy, or
 - iii) Such use does not conflict with any non-disclosure agreement, or term thereof, by and between the State and Vendor or Vendor's personnel.
 - d) Unless otherwise provided by the Agency, the Vendor shall furnish all necessary personnel, Services, and otherwise perform all acts, duties and responsibilities necessary or incidental to the accomplishment of the tasks specified in the Agreement. The Vendor shall be legally and financially responsible for its personnel including, but not limited to, any deductions for social security and other withholding taxes required by state or federal law. The Vendor shall be solely responsible for acquiring any equipment, furniture, and office space not furnished by the State necessary for the Vendor to comply with the Agreement. The Vendor personnel shall comply with any applicable State facilities or other security rules and regulations.
- 4) **PERSONAL SERVICES**: The State shall have and retain the right to obtain personal Services of any individuals providing Services under the Agreement. This right may be exercised at the State's discretion in the event of any transfer of the person providing personal Services, termination, default, merger, acquisition, bankruptcy or receivership of the Vendor to ensure continuity of Services provided under the Agreement. Provided, however, that the Agency shall not retain or solicit any Vendor employee for purposes other than completion of personal Services due as all or part of any performance due under the Agreement.
- a) Vendor personnel shall perform any duties on the premises of the State during the State's regular work days and normal work hours, except as may be specifically agreed otherwise, established in the specification, or statement of work.
 - b) The State has and reserves the right to disapprove the continuing assignment of Vendor personnel provided by Vendor under the Agreement. If this right is exercised and the Vendor is not able to replace the disapproved personnel as required by the State, the parties agree to employ best commercial efforts to informally resolve such failure equitably by adjustment of other duties, set-off, or modification to other terms that may be affected by Vendor's failure.
 - c) Vendor will make every reasonable effort consistent with prevailing business practices to honor the specific requests of the State regarding assignment of Vendor's employees. Vendor reserves the sole right to determine the assignment of its employees. If one of Vendor's employees is unable to

perform due to illness, resignation, or other factors beyond Vendor's control, Vendor will provide suitable personnel at no additional cost to the State.

- d) The Agreement shall not prevent Vendor or any of its personnel supplied under the Agreement from performing similar Services elsewhere or restrict Vendor from using the personnel provided to the State, provided that:
 - i) Such use does not conflict with the terms, specifications or any amendments to the Agreement, or
 - ii) Such use does not conflict with any procurement law, regulation or policy, or
 - iii) Such use does not conflict with any non-disclosure agreement, or term thereof, by and between the State and Vendor or Vendor's personnel.

Section 4: Terms and Conditions Applicable to Information Technology Goods and Services

- 1) **SOFTWARE LICENSE FOR HARDWARE, EMBEDDED SOFTWARE AND FIRMWARE:** Deliverables comprising goods, equipment or products (hardware) may contain software for internal operation, or as embedded software or firmware that is generally not sold or licensed as a severable software product. Software may be provided on separate media, such as a CD-ROM or other media, or may be included within the hardware at or prior to delivery. Such software is proprietary, copyrighted, and may also contain valuable trade secrets and may be protected by patents. Vendor grants the State a license to use the Code (or any replacement provided) on, or in conjunction with, only the Deliverables purchased, or with any system identified in the solicitation documents. The State shall have a worldwide, nonexclusive, non-sublicensable license to use such software and/or documentation for its internal use. The State may make and install copies of the software to support the authorized level of use. Provided, however that if the hardware is inoperable, the software may be copied for temporary use on other hardware. The State shall promptly affix to any such copy the same proprietary and copyright notices affixed to the original. The State may make one copy of the software for archival, back-up or disaster recovery purposes. The license set forth in this Paragraph shall terminate immediately upon the State's discontinuance of the use of all equipment on which the software is installed. The software may be transferred to another party only with the transfer of the hardware. If the hardware is transferred, the State shall i) destroy all software copies made by the State, ii) deliver the original or any replacement copies of the software to the transferee, and iii) notify the transferee that title and ownership of the software and the applicable patent, trademark, copyright, and other intellectual property rights shall remain with Vendor, or Vendor's licensors. The State shall not disassemble, decompile, reverse engineer, modify, or prepare derivative works of the embedded software, unless permitted under the solicitation documents.
- 2) **LICENSE GRANT FOR APPLICATION SOFTWARE, (COTS):** This paragraph recites the scope of license granted, if not superseded by a mutually agreed and separate licensing agreement, as follows:
 - a) Vendor grants to the State, its Agencies and lawful customers a non-exclusive, non-transferable and non-sublicensable license to use, in object code format, Vendor's software identified in the solicitation documents, Vendor's Statement of Work (SOW), or an Exhibit thereto executed by the parties ("Software"), subject to the restrictions set forth therein, such as the authorized computer system, the data source type(s), the number of target instance(s) and the installation site. Use of the Software shall be limited to the data processing and computing needs of the State, its Agencies and lawful customers. This license shall be perpetual unless terminated as provided herein. The State agrees not to distribute, sell, sublicense or otherwise transfer copies of the Software or any portion thereof. For purposes of this Agreement, a State Entity shall be defined as any department or agency of the State of North Carolina, which is controlled by or under common control of the State or who is a lawful customer of the State pursuant to Article 3D of Chapter 147 of the General Statutes.
 - b) Vendor shall provide all encryption or identification codes or authorizations that are necessary or proper for the operation of the licensed Software.

- c) The State shall have the right to copy the Software, in whole or in part, for use in conducting benchmark or acceptance tests, for business recovery and disaster recovery testing or operations, for archival or emergency purposes, for back up purposes, for use in preparing derivative works if allowed by the solicitation documents or statements of work, or to replace a worn copy.
 - d) The State may modify non-personal Software in machine-readable form for its internal use in merging the same with other software program material. Any action hereunder shall be subject to uses described in this paragraph, the restrictions imposed by Paragraph 3), and applicable terms in the solicitation documents or statements of work.
- 3) **WARRANTY TERMS:** Notwithstanding anything in the Agreement or Exhibit hereto to the contrary, Vendor shall assign warranties for any Deliverable supplied by a third party to the State.
- a) a) Vendor warrants that any Software or Deliverable will operate substantially in conformity with prevailing specifications as defined by the current standard documentation (except for minor defects or errors which are not material to the State) for a period of ninety (90) days from the date of acceptance ("Warranty Period"), unless otherwise specified in the Solicitation Documents. If the Software does not perform in accordance with such specifications during the Warranty Period, Vendor will use reasonable efforts to correct any deficiencies in the Software so that it will perform in accordance with or substantially in accordance with such specifications.
 - b) Vendor warrants to the best of its knowledge that:
 - i) The licensed Software and associated materials do not infringe any intellectual property rights of any third party;
 - ii) There are no actual or threatened actions arising from, or alleged under, any intellectual property rights of any third party;
 - iii) The licensed Software and associated materials do not contain any surreptitious programming codes, viruses, Trojan Horses, "back doors" or other means to facilitate or allow unauthorized access to the State's information systems.
 - iv) The licensed Software and associated materials do not contain any timer, counter, lock or similar device (other than security features specifically approved by Customer in the Specifications) that inhibits or in any way limits the Software's ability to operate.
 - c) UNLESS MODIFIED BY AMENDMENT OR THE SOLICITATION DOCUMENTS, THE WARRANTIES IN THIS PARAGRAPH ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, OR WHETHER ARISING BY COURSE OF DEALING OR PERFORMANCE, CUSTOM, USAGE IN THE TRADE OR PROFESSION OR OTHERWISE, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NO OTHER REPRESENTATIONS OR WARRANTIES HAVE FORMED THE BASIS OF THE BARGAIN HEREUNDER.
- 4) **RESTRICTIONS:** State's use of the Software is restricted as follows:
- a) The license granted herein is granted to the State and to any political subdivision or other entity permitted or authorized to procure Information Technology through the Department of Information Technology. If the License Grant and License Fees are based upon the number of Users, the number of Users may be increased at any time, subject to the restrictions on the maximum number of Users specified in the solicitation documents.
 - b) No right is granted hereunder to use the Software to perform Services for commercial third parties (so-called "service bureau" uses). Services provided to other State Departments, Agencies or political subdivisions of the State is permitted.
 - c) The State may not copy, distribute, reproduce, use, lease, rent or allow access to the Software except as explicitly permitted under this Agreement, and State will not modify, adapt, translate, prepare derivative works (unless allowed by the solicitation documents or statements of work,) decompile, reverse engineer, disassemble or otherwise attempt to derive source code from the Software or any internal data files generated by the Software.
 - d) State shall not remove, obscure or alter Vendor's copyright notice, trademarks, or other proprietary rights notices affixed to or contained within the Software.

- 5) **SUPPORT OR MAINTENANCE SERVICES**: This paragraph recites the scope of maintenance Services due under the license granted, if not superseded by a separate licensing and maintenance agreement or as may be stated in the solicitation documents. Subject to payment of a Support Service or Maintenance Fee stated in the solicitation documents for the first year and all subsequent years, if requested by the State, Vendor agrees to provide the following support Services ("Support Services") for the current version and one previous version of the Software commencing upon delivery of the Software:
- a) **Error Correction**: If the error conditions reported by the State pursuant to the General Terms and Conditions are not corrected in a timely manner, the State may request a replacement copy of the licensed Software from Vendor. In such event, Vendor shall then deliver a replacement copy, together with corrections and updates, of the licensed Software within 24 hours of the State's request at no added expense to the State.
 - b) **Other Agreement**: This Paragraph 5 may be superseded by written mutual agreement provided that: Support and maintenance Services shall be fully described in such a separate agreement annexed hereto and incorporated herein
 - c) **Temporary Extension of License**: If any licensed Software or CPU/computing system on which the Software is installed fails to operate or malfunctions, the term of the license granted shall be temporarily extended to another CPU selected by the State and continue until the earlier of:
 - i) Return of the inoperative CPU to full operation, or
 - ii) Termination of the license.
 - d) **Encryption Code**: Vendor shall provide any temporary encryption code or authorization necessary or proper for operation of the licensed Software under the foregoing temporary license. The State will provide notice by expedient means, whether by telephone, e-mail or facsimile of any failure under this paragraph. On receipt of such notice, Vendor shall issue any temporary encryption code or authorization to the State within twenty-four (24) hours; unless otherwise agreed.
 - e) **Updates**: Vendor shall provide to the State, at no additional charge, all new releases and bug fixes (collectively referred to as "Updates") for any Software Deliverable developed or published by Vendor and made generally available to its other customers at no additional charge. All such Updates shall be a part of the Program and Documentation and, as such, be governed by the provisions of the Agreement.
 - f) **Telephone Assistance**: Vendor shall provide the State with telephone access to technical support engineers for assistance in the proper installation and use of the Software, and to report and resolve Software problems, during normal business hours, 7:30 AM - 5:30 PM Eastern Time, Monday-Friday. Vendor shall respond to the telephone requests for Program maintenance service, within four (4) business hours

ATTACHMENT C: DESCRIPTION OF OFFEROR

Provide the information about the offeror.

Offeror's full name	
Offeror's address	
Offeror's telephone number	
Ownership	☐ Public ☐ Partnership ☐ Subsidiary ☐ Other (specify)
Date established	
If incorporated, State of incorporation.	
North Carolina Secretary of State Registration Number, if currently registered	
Number of full-time employees on January 1 st for the last three years or for the duration that the Vendor has been in business, whichever is less.	
Offeror's Contact for Clarification of offer: Contact's name Title Email address and Telephone Number	
Offeror's Contact for Negotiation of offer: Contact's name Title Email address and Telephone Number	
If Contract is Awarded, Offeror's Contact for Contractual Issues: Contact's name Title Email address and Telephone Number	
If Contract is Awarded, Offeror's Contact for Technical Issues: Contact's name Title Email address and Telephone Number	

HISTORICALLY UNDERUTILIZED BUSINESSES

Historically Underutilized Businesses (HUBs) consist of minority, women and disabled business firms that are at least fifty-one percent owned and operated by an individual(s) of the categories. Also included as HUBs are disabled business enterprises and non-profit work centers for the blind and severely disabled.”

Pursuant to N.C.G.S. §§ 143B-1361(a), 143-48 and 143-128.4, the State invites and encourages participation in this procurement process by businesses owned by minorities, women, disabled, disabled business enterprises and non-profit work centers for the blind and severely disabled. This includes utilizing subcontractors to perform the required functions in this RFP. Contact the North Carolina Office of historically Underutilized Businesses at 919-807-2330 with questions concerning NC HUB certification. <http://ncadmin.nc.gov/businesses/hub>

Respond to the questions below.

1. Is Vendor a Historically Underutilized Business? ☐ Yes ☐ No
2. Is Vendor Certified with North Carolina as a Historically Underutilized Business? ☐ Yes ☐ No

If so, state HUB classification:

ATTACHMENT D: COST FORM

Vendors will submit all Crossroads pricing with the technical response, but in a separate area that allows cost and pricing information to be partitioned separately from other documents. All electronic submission forms will also separate the cost and pricing from the technical proposals.

Total Cost Summary: Vendors will include a Total Cost Summary Table in addition to the costs provided in each of the detailed cost tables. The Total Cost Summary Table will include total cost including all deliverables, with the exception of optional services. The evaluation of cost proposal responses will be based on the Table 1 summary table. Vendors are responsible for ensuring that the Total Cost Summary Table accurately reflects the cost in each of the individual pricing tables

Cost Table 1 - Total Cost of Contract

Description	Total Cost
Transition-In Phase Cost (from Cost Table 2)	\$
Total Annual M&E Phase Cost – Contract Years 1-10 (from Cost Table 3)	\$
Total Annual Hosting Costs – Contract Years 1-10 (from Cost Table 4)	\$
Transition-Out Period Cost (from Cost Table 5)	\$
Total Document Deliverable Cost (from Cost Table 6)	\$
Supplemental Services Hours Contract Years 1-10 (from Cost Table 7)	\$
Total Ten-Year Cost	\$

Cost Table 1a. Total Cost by Contract Term

Contract Term	Total Cost
Initial seven (7) year Contract Term	
Optional Renewal Term 1 (Contract year 8)	
Optional Renewal Term 2 (Contract year 9)	
Optional Renewal Term 3 (Contract year 10)	
Total Contract Cost including Optional Renewal Terms	

1.1. Price for Crossroads Transition-In, Annual Maintenance, and Transition-Out

Provide the Vendor's proposed maintenance pricing for each year of the Contract, not including the Supplemental Service Hours.

Cost Table 2 - Pricing for Transition-In Phase (Deliverables 1.x)

Transition-In Month	Monthly Transition-In Cost
Month 1	\$
Month 2	\$
Month 3	\$
Month 4	\$
Month 5	\$
Month 6	\$
Month 7	\$
Month 8	\$
Total Transition-In Phase Cost	\$

Cost Table 3 - Pricing for Crossroads Annual Maintenance and Enhancement Phase (Deliverables 6.x)

Description	Monthly M&E Cost	Multiplier	Total Fixed Annual M&E Cost
Contract Year 1	\$	4	\$
Contract Year 2	\$	12	\$
Contract Year 3	\$	12	\$
Contract Year 4	\$	12	\$
Contract Year 5	\$	12	\$
Contract Year 6	\$	12	\$
Contract Year 7	\$	12	\$
Optional Contract Year 8	\$	12	\$
Optional Contract Year 9	\$	12	\$
Optional Contract Year 10	\$	12	\$
Total Ten Year M&E Phase Cost			\$

Cost Table 4 - Pricing for Crossroads Annual Hosting (Deliverables 21.x)

Description	Monthly or Annual Hosting Cost	Multiplier	Total Fixed Annual Hosting Cost
Contract Year 1	\$	4 mo	\$
Contract Year 2	\$	12 mo or 1 yr	\$
Contract Year 3	\$	12 mo or 1 yr	\$
Contract Year 4	\$	12 mo or 1 yr	\$
Contract Year 5	\$	12 mo or 1 yr	\$
Contract Year 6	\$	12 mo or 1 yr	\$
Contract Year 7	\$	12 mo or 1 yr	\$
Optional Contract Year 8	\$	12 mo or 1 yr	\$
Optional Contract Year 9	\$	12 mo or 1 yr	\$
Optional Contract Year 10	\$	12 mo or 1 yr	\$
Total Ten Year Hosting Cost			\$

Cost Table 5 - Pricing for Transition-Out Period – Fixed Amount (Deliverable 16)

Transition-Out Period (inclusive of completion of all Transition-Out Period tasks and submission of the Transition-Out Completion Report)	\$

1.2. Price for Crossroads Deliverables

There are deliverables that are needed to ensure a successful release deployments and operations of the NC WIC Crossroads System. Payment will only be made for the deliverables listed below after unconditional acceptance by the State. Acceptance by the State will be in the form of a written acknowledgement that the Deliverable meets the requirements. Provide the Vendor's proposed pricing for each of the deliverables listed in Price Table 6 below.

Cost Table 6 - Pricing for Product Deliverables

Deliverable ID	Deliverable Name	Price
3B	Work Plan and Schedule FINAL	\$
9	Production Deployment Plan	\$
Total Deliverable Cost		\$

1.3. Supplemental Services

The State will require the Vendor to provide Supplemental Services, for completion and deployment of Changes Requests. Vendors will provide Change Request cost estimates using the blended hourly resource pricing for each of the Contract Years one (1) through seven (7) and optional years one (1) through three (3) in Price Table 7 below. Hours are invoiced as utilized in accordance with the Change Request process.

Cost Table 7 - Pricing of Supplemental Services

Description	# Change Request Hours	Blended Hourly Rate	Total Cost
Contract Years 1-7	3500	\$	\$
Optional Contract Year 8	500	\$	\$
Optional Contract Year 9	500	\$	\$
Optional Contract Year 10	500	\$	\$
Total Ten Year Supplemental Services Cost			\$

1.4. Other Optional Services

Vendors are encouraged to propose other optional technical services that may improve efficiency and/or effectiveness to the Crossroads system, its interfaces to 3rd party solutions, or NC WIC Program as a whole. For example, vendors may propose an optional service for a mobile phone application, to be used by participants to access benefit and other WIC information, and/or other optional services that may be beneficial to the program and stakeholders.

Optional services may be bid to be implemented upon contract award or may be initiated in any of the contract years. The Other Optional Services must be compliant with all security and enterprise specifications under Section 3.0, described in enough detail for North Carolina to evaluate the services, and any associated pricing will be separate from the pricing for the Crossroads Scope of Work sections. A narrative description will be provided for each optional service, including a description, information on

other states' programs that have implemented the service, why it would be advantageous for NC, and the cost broken out by industry standards and/or monthly/annually, as applicable. Each optional service must be included separately in the narrative and cost proposal.

Vendors may add as many rows as needed to Cost Table 8 for optional services proposed, and may include annual pricing. The State must not be charged for any optional services unless such optional services are specifically requested by the State in writing.

Cost Table 8 - Proposed Optional Services Pricing

Optional Service Proposed	Pricing
Optional Service 1:	\$
Optional Service 2:	\$
Optional Service 3:	\$
Optional Service 4:	\$

ATTACHMENT E: VENDOR CERTIFICATION FORM

1) ELIGIBLE VENDOR

The Vendor certifies that in accordance with N.C.G.S. §143-59.1(b), Vendor is not an ineligible vendor as set forth in N.C.G.S. §143-59.1 (a).

The Vendor acknowledges that, to the extent the awarded contract involves the creation, research, investigation or generation of a future RFP or other solicitation; the Vendor will be precluded from bidding on the subsequent RFP or other solicitation and from serving as a subcontractor to an awarded vendor.

The State reserves the right to disqualify any bidder if the State determines that the bidder has used its position (whether as an incumbent Vendor, or as a subcontractor hired to assist with the RFP development, or as a Vendor offering free assistance) to gain a competitive advantage on the RFP or other solicitation.

2) CONFLICT OF INTEREST

Applicable standards may include: N.C.G.S. §§143B-1352 and 143B-1353, 14-234, and 133-32. The Vendor shall not knowingly employ, during the period of the Agreement, nor in the preparation of any response to this solicitation, any personnel who are, or have been, employed by a Vendor also in the employ of the State and who are providing Services involving, or similar to, the scope and nature of this solicitation or the resulting contract.

3) E-VERIFY

Pursuant to N.C.G.S. § 143B-1350(k), the State shall not enter into a contract unless the awarded Vendor and each of its subcontractors comply with the E-Verify requirements of N.C.G.S. Chapter 64, Article 2. Vendors are directed to review the foregoing laws. Vendors claiming exceptions or exclusions under Chapter 64 must identify the legal basis for such claims and certify compliance with federal law regarding registration of aliens including 8 USC 1373 and 8 USC 1324a. Any awarded Vendor must submit a certification of compliance with E-Verify to the awarding agency, and on a periodic basis thereafter as may be required by the State.

4) CERTIFICATE TO TRANSACT BUSINESS IN NORTH CAROLINA

As a condition of contract award, awarded Vendor shall have registered its business with the North Carolina Secretary of State and shall maintain such registration throughout the term of the Contract.

Signature: _____ Date: _____

Printed Name: _____ Title: _____

ATTACHMENT F: LOCATION OF WORKERS UTILIZED BY VENDOR

In accordance with N.C.G.S. §143B-1361(b), Vendor must identify how it intends to utilize resources or workers located outside the U.S., and the countries or cities where such are located. The State will evaluate additional risks, costs, and other factors associated with the Vendor's utilization of resources or workers prior to making an award for any such Vendor's offer. The Vendor shall provide the following:

- a) The location of work to be performed by the Vendor's employees, subcontractors, or other persons, and whether any work will be performed outside the lower 48 contiguous United States. The Vendor shall provide notice of any changes in such work locations if the changes result in performing work outside of the contiguous United States.
- b) Any Vendor or subcontractor providing support or maintenance Services for software, call or contact center Services shall disclose the location from which the call or contact center Services are being provided upon request.

Will Vendor perform any work outside of the contiguous United States?

☐ YES ☐ NO

If yes, Vendor MUST list what countries the employees are working and in what capacity are they accessing State Data. Specifically, the State must know if the employees are Help Desk support, Technical Support and/or Coder, etc.

ATTACHMENT G: REFERENCES

The Vendor shall provide three (3) references of customers utilizing the proposed solution fully implemented in a setting similar to this solicitation's scope of work. References within like North Carolina communities / industries are encouraged.

The Vendor should have implemented the respective proposed service within the last three (3) years. Customer references whose business processes and data needs are similar to those performed by the Agency needing this solution in terms of functionality, complexity, and transaction volume are encouraged.

For each reference, the Vendor shall provide the following information:

- a. Customer name.
- b. Customer address.
- c. Current telephone number of a customer employee most familiar with the offered solution implementation.
- d. Customer email address
- e. Time period over which each offered solution implementation was completed.
- f. Brief summary of the offered solution implementation.
- g. List of offered solution products installed and operational.
- h. Number of vendor or technical staff supporting, maintaining and managing the offered solution
- i. Number of end users supported by the offered solution.
- j. Number of sites supported by the offered solution.

ATTACHMENT H: FINANCIAL REVIEW FORM

Vendor shall review the Financial Review Form, provide responses in the gray-shaded boxes, and submit the completed Form as an Excel file with its offer. Vendor shall not add or delete rows or columns in the Form, or change the order of the rows or column in the file.

1. Vendor Name:
2. Company structure for tax purposes (C Corp, S Corp, LLC, LLP, etc.):
3. Have you been in business for more than three years? ☐ Yes ☐ No
4. Have you filed for bankruptcy in the past three years? ☐ Yes ☐ No
5. In the past three years, has your auditor issued any notification letters addressing significant issues? If yes, please explain and provide a copy of the notification letters. ☐ Yes ☐ No
6. Are the financial figures below based on audited financial statements? ☐ Yes ☐ No
7. Start Date of financial statements:
End Date of financial statements:
8. Provide a link to annual reports with financial statements and management discussion for the past three complete fiscal years:
9. Provide the following information for the past three complete fiscal years:

	Latest complete fiscal year minus two years	Latest complete fiscal year minus one year	Latest complete fiscal year
BALANCE SHEET DATA			
a. Cash and Temporary Investments			
b. Accounts Receivable (beginning of year)			
c. Accounts Receivable (end of year)			
d. Average Account Receivable for the Year (calculated)			
e. Inventory (beginning of year)			
f. Inventory (end of year)			
g. Average Inventory for the Year (calculated)			
h. Current Assets			
i. Current Liabilities			
j. Total Liabilities			
k. Total Stockholders' Equity (beginning of year)			
l. Total Stockholders' Equity (end of year)			
m. Average Stockholders' Equity during the year (calculated)			
INCOME STATEMENT DATA			
a. Net Sales			
b. Cost of Goods Sold (COGS)			
c. Gross Profit (Net Sales minus COGS) (calculated)			
d. Interest Expense for the Year			
e. Net Income after Tax			
f. Earnings for the Year before Interest & Income Tax Expense			
STATEMENT OF CASH FLOWS			
a. Cash Flow provided by Operating Activities			
b. Capital Expenditures (property, plant, equipment)			

ATTACHMENT K. FEDERAL AND OTHER STATE SPECIFICATIONS

The following provisions govern this product and the related technical requirements. Keep these in mind when preparing the Vendor's response

FNS HANDBOOK 901 PROVISIONS AND OTHER FEDERAL PROCUREMENT REQUIREMENTS

- a) No component or documentation of the Crossroads system will be in the public domain.
- b) Federal regulations 2 CFR § 200.315 provides for title to intangible property acquired under a Federal award. This regulation is located at the following website <https://www.ecfr.gov> .

The regulation includes that FNS reserves a royalty-free, nonexclusive, and irrevocable license to reproduce, publish, or otherwise use and to authorize others to use for Federal government purposes, the North Carolina Crossroads software and modifications thereof, and associated documentation designed, developed, or installed with Federal financial participation.
- c) Federal regulations 2 CFR § 200.317 (Procurement by states). This regulation is located at the following website <https://www.ecfr.gov> , and includes a list of provisions under 2 CFR 200 Appendix II that must be included in this RFP.
- d) Federal regulations 2 CFR Part 416 (Special Procurement Provisions). This regulation is located at the following website <https://www.ecfr.gov> , and includes exclusions on prospective contractors that also develop procurement documentation related to this RFP.
- e) Federal regulations 2 CFR § 421.10 (Drug-Free Workplace Act). This regulation is located at the following website <https://www.ecfr.gov> , and includes USDA policies and procedures for compliance with the Act.
- f) Federal regulations 28 CFR Part 35 (Americans with Disabilities Act). This regulation is located at the following website <https://www.ecfr.gov> , and implements Subtitle A of Title II of the Americans with Disabilities Act.

FNS APPROVAL

- a) This Crossroads RFP and resulting Contract is dependent upon FNS approval. Delays in approval may impact the timeline and schedule for Contract execution.

COMPLY WITH STATE CIO / DIT / ITD REQUESTS FOR ADDITIONAL SUPPORT

- a) If requested by the State, the Vendor will be required to support, at no additional cost, product reviews and assessments, various risk management, problem or issue resolution or other requests regarding WIC Crossroads from the State Chief Information Officer (CIO), the Department of Information Technology (DIT), and the DHHS Information Technology Division (ITD).
- b) In the event the State of North Carolina declares an emergency or disaster at the county, geographic region, or statewide level, the Vendor will assist the State as requested in restoring the State production system or implementing any emergency software modifications needed to minimize impact to participants of Crossroads programs.

VENDOR SITE VISITS

- a) The State's designated representative(s) and/or FNS may visit the Vendor's site(s) at any time with twenty-four (24) hour notice.

COMPLIANCE WITH STANDARDS, OPERATIONAL SPECIFICATIONS, AND FNS REQUIREMENTS

- a) Crossroads will remain compliant with the most recent version of the following standards and specifications
 - Software development best practices and standards such as the Agile methodology.
 - The FNS Operating Rules for WIC EBT systems as defined by USDA/FNS.
 - The FNS Technical Implementation Guide (TIG)
 - The FNS WIC Universal MIS-EBT Interface (WUMEI)
 - The NC Technical Architecture System Design (TASD)
 - The FNS Handbook 901
- b) Each major release of Crossroads will contain a mutually agreed number of Change Request hours, and a mutually agreed number of defect corrections, for the Vendor to meet the SLA.
- c) Vendor will furnish the necessary staff, material, travel expenses, software licenses, digital certificates, equipment, services, and facilities to perform the work described in this RFP. The State's designee(s), including auditors, and/or FNS may visit the Vendor's site(s) as stipulated under Attachment K.
- d) All Vendor / sub-contractor staff (including but not limited to software development, build, test, installation, help desk, product management, etc.), facilities, and equipment including all databases, servers and workstations (such as environments for software development, build, test, etc.) and tools (such as FTP storage sites, cloud hosting sites, issue reporting systems, etc.) will be physically located in the continental United States.

Only Vendor / sub-contractor staff physically located in the United States, including its territories, will administer equipment servers and tools.

STATE OF NORTH CAROLINA
Department of Health and Human Services
Division of Child and Family Well-Being

Maintenance and Enhancement Services
for the Crossroads WIC Management Information
System

RFP No. 30-25002-DCFW
Thursday March 6, 2025 at 2PM EDT
Technical Response Document

Submitted By:

GCOM SOFTWARE LLC D/B/A VOYATEK

Corporate Headquarters
9175 Guilford Road, Suite 218, Columbia, MD 21046

Jay Saunders, Vice President
RFP@voyatek.com | (913) 707-0389



Contents

Introduction and Executive Summary	1
a) Signed Execution Page & Solicitation	5
Attachment A – Definitions.....	6
Attachment B – Department of Information Technology Terms and Conditions for Vendor Hosted Solutions.....	7
Attachment C – Description of Offeror	8
Attachment D – Cost Form	9
Attachment E – Vendor Certification Form	10
Attachment F – Location of Workers Utilized	11
Attachment G – References	12
Attachment H – Financial Review Form.....	13
b) Requirements and Specifications (Chapter 3 in RFP).....	14
3.1 General Requirements and Specifications	14
3.2 Security Specifications.....	15
3.3 Enterprise Specifications	17
3.4 Business and Technical Requirements	18
3.4.1 System	19
3.4.2 Other Maintenance Tasks.....	20
3.4.3 Product Deliverables	23
3.5 Business and Technical Specifications	27
3.5.1 Scope	27
3.5.2 Objectives	34
3.5.3 Product Management.....	40
3.5.4 Coordination with WIC EBT Provider / Interface with the EBT System	63
3.5.5 Coordination with EBT FMNP Provider	67
3.5.6 Production and Non-Production Data Centers.....	67
3.5.7 Help Desk Services.....	78
3.5.8 Issue Identification and Correction from UAT and Production	81

3.5.9 Installation Support for New Builds	99
3.5.10 Deployment of Releases for Statewide Production	102
3.5.11 System Training	107
3.5.12 Change Request Process.....	108
3.5.13 Technical Upgrades and Environment Validation.....	117
3.5.14 Contract Transition-Out Procedures	119
3.5.15 North Carolina WIC Program and FMNP Program Data.....	121
3.5.16 Supplemental Services.....	122
c) Security Vendor Readiness Assessment Report (VRAR).....	123
d) Architecture Diagrams.....	124
e) Detailed Project Timeline	127
f) Errata and Exceptions – Exceptions to Requirements and Specifications	129
g) Vendor's License and Maintenance Agreements.....	132
h) Other Supporting Materials	133
Appendices	134
Appendix A: Transition-In Plan	135
Appendix B: Product Management Plan.....	136
Appendix C: Product Work Plan and Schedule	137
Appendix D: Quality Assurance Management Plan.....	138
Appendix E: Rehosting Implementation and Rollout Plan.....	139
Appendix F: Disaster Recovery and Contingency Plan	140
Appendix G: Security and Vulnerability Plan	141
Appendix H: Risks and Issues Management Plan	142
Appendix J: Configuration Management / Release Management Plan	143
Appendix K: Evidence of Vendor Financial Stability	144
Appendix L: Transition-Out Plan.....	145
Appendix M: Partnerships and Contractual Relationships	146
Appendix N: Help Desk Plan	147
Appendix P: Communication and Coordination Plan	148
Appendix Q: SOC 2.....	149

Appendix R: Optional Services	150
Data & Reporting Analyst.....	150
Supplemental Development Capacity.....	150
Mobile Application.....	151
Farmers Market	168
Penetration Testing.....	173
TeleWIC / Two-way Texting.....	174
Appendix S: Key Personnel Resumes.....	176
M&E Vendor Product Manager – Jennifer Saunders.....	176
M&E Vendor Development Manager – Michael Heinrich	177
M&E Vendor Test Manager – Helena Young.....	178
M&E Vendor Business Analyst Manager – Cindy Kochersperger.....	179
M&E Vendor Advisory Technical Architect – Jon Moreau	180

Figures

Figure 1: Voyatek's Nutrition Practice Organization Chart	41
Figure 2: Voyatek's WIC Cascades Product Team Organization Chart	48
Figure 3: Voyatek Team Test Phases.....	82
Figure 4: Data Scope by Test Phase / Environment.....	87
Figure 5: Sample DevOps Project Dashboard.....	95
Figure 6: Release Pipeline with Pending Approval for Customer Environment Deployment.....	102
Figure 7: Crossroads Azure Network Architecture	124
Figure 8: Technology Stack Diagram.....	125
Figure 9: Data Communication Diagram.....	126
Figure 10: Detailed Project Timeline.....	128
Figure 11: Mobile App Can be Branded Using North Carolina Colors and Images	151
Figure 12: Participants Login or Register on the Mobile App	153
Figure 13: Mobile App Locator for WIC Clinics and Authorized Vendors	154
Figure 14: Mobile App Menu and Home Page	155

Figure 15: Mobile App Appointments.....	156
Figure 16: Mobile app Benefit Balance Screens	157
Figure 17: Mobile App UPC Scanning Tool	158
Figure 18: Mobile App Supports Access to North Carolina WIC Resource Links.....	159
Figure 19: Mobile App Document Upload.....	161
Figure 20: Mobile App Appointment Method Indicator	162
Figure 21: Mobile App Product Submission Functions	163
Figure 22: Mobile App Multiple eWIC Card Management.....	164
Figure 23: Mobile App Signature Capture	165
Figure 24: Mobile Application Nutrition Education System.....	166
Figure 25: Mobile App Redemption Dashboard	167
Figure 26: Farmers Market Home Screen	169
Figure 27: Farmers Market Available Balance.....	170
Figure 28: Farmers Market Summary Screen.....	171
Figure 29: The Farmers Market Daily Report	172

Tables

Table 1: Other Maintenance Tasks	20
Table 2: RFP Table 1 List of Product Deliverables.....	25
Table 3: Voyatek Experience Serving the WIC Community.....	63
Table 4: Voyatek Test Phases	82
Table 5: Interface Partners by Type of Interface	88
Table 6: System Testing Topics for Grouping Tests and Issues	90
Table 7: Defect / Issue Classification Criteria	95
Table 8: Change Request Process – Roles and Responsibilities	109
Table 9: Defect Resolution Time by Priority Level.....	115

Introduction and Executive Summary

In 2023 GCOM Software merged with OnCore Consulting to form a nationwide large-scale digital software and solutions company focused solely on the public sector market, providing outcome-driven solutions and services. **As of April 1, 2024, we are now Voyatek and operating under the new brand. We are passionate about delivering outcomes to our government clients through our innovative solutions.** Voyatek currently serves clients in 32 states, supporting departments and agencies that serve much of our nation's population. Our mission is to provide governments with innovative, modern technology solutions for efficient and improved constituent services. We specialize in nutrition, public health, public safety, taxation, licensing and permitting, and digital identity. In 2018, we acquired 3Sigma Software, the leading provider of WIC MIS system solutions and support nationally. 3Sigma's investment in nutrition solutions spans two decades of WIC MIS solution innovation and leadership.

Voyatek is today the leading provider of maintenance and enhancement (M&E) services for WIC MIS systems, providing support for multiple versions of the Crossroads WIC MIS and the WoW (WIC On the Web) WIC MIS across 14 states and numerous other smaller state agencies. This proposal will demonstrate that Voyatek is the right choice for the next era of M&E support for the North Carolina Crossroads WIC MIS.

Voyatek is the best company to partner with North Carolina WIC for the following reasons:

- ✓ **Commitment to Public Health:** Voyatek is committed to supporting state and local governments nationwide with innovative, modern technology solutions that are vital to keep agencies running efficiently and to improve participant experience. We deliver our solutions to the public sector, with a focus on modernizing and enhancing legacy IT systems in nutrition, public health, public safety, licensing and permitting, and cybersecurity markets. By selecting Voyatek, North Carolina continues with a partner focused on the mission of government and WIC to serve the country's participants.
- ✓ **WIC Dedication:** Voyatek's Nutrition Practice continues to grow and increase the depth of our WIC experience. Many team members have 20-30 years of individual experience supporting WIC that translates to a deep understanding of the challenges facing the WIC program today and how to leverage technology to solve problems. For example, Voyatek's TeleWIC solution revolutionizes the delivery of WIC services by reducing the travel burden on participants and their children through video conference appointments and thereby enabling states to reach more clients in need of WIC services and benefits. Over 50% of WIC participants are served using systems developed or maintained by Voyatek.
- ✓ **North Carolina Expertise:** As the current provider of Crossroads WIC MIS M&E services for NC WIC, Voyatek is uniquely qualified to provide the expertise North Carolina is seeking. Our

understanding of the NC WIC program practices, standards, preferences, and Crossroads enable our team to seamlessly transition to the next phase of M&E support.

- ✓ Crossroads Expertise: Voyatek's Nutrition Practice includes many team members who worked with North Carolina to design and develop Crossroads, *many of whom have been supporting NC WIC for the past six years and who Voyatek is proposing to continue supporting the State for the next phase of the Crossroads evolution.*
 - Jay Saunders, one of the original Crossroads project managers, leads Voyatek's Nutrition Product Development team which is currently developing our next generation WIC MIS.
 - Jon Moreau, the Crossroads technical architect, is currently designing and developing the next generation of WIC MIS architecture.
 - Ryan Buysse, the original Crossroads solution architect, provides WIC innovation and thought leadership for the development of our next generation WIC MIS platform.
 - Cindy Kochersperger & Helena Young, the original Crossroads lead business analyst and quality assurance lead, respectively, continue to support the system for North Carolina.
 - Keith Myles, NC Crossroads senior developer, supported the Washington Crossroads system before working for NC and has expanded his experience to support the Crossroads User Group.

These Crossroads alumni form the basis of Voyatek's Crossroads Practice, dedicated to excellence in the Crossroads product. They continue to cross-train our growing team of Crossroads professionals. Last year we were selected to support the Crossroads User Group and last month we were awarded the support for the Washington WIC Cascades (Crossroads) MIS. We are excited to begin working with another version of this sophisticated WIC MIS. *Voyatek is proud of our ability to steward these three versions of Crossroads, enabling collaboration and sharing between their respective state agencies.*

- ✓ Cloud Experience: As North Carolina prepares to transition the hosting of Crossroads to the cloud, Voyatek will be an excellent partner to lead and support the rehosting initiative. We have extensive experience in developing and maintaining cloud-based systems for our government clients. Our Information Technology Services & Security organization consists of a dedicated team responsible for the maintenance, monitoring, and security of all environments. This team operates a 24x7 Service Operations Center to provide continuous monitoring of all cloud environments, including tenants in both Amazon Web Services (AWS) and Microsoft Azure across multiple regions, ensuring maximum scalability and uptime. Specifically, our Nutrition Practice maintains tenants in Azure Commercial Cloud, adhering to a 100% compliant SOC 2 audit standard. Recently, we successfully transitioned Rhode Island Crossroads to Azure and will replicate this approach for NC WIC when migrating the

Crossroads system to Azure. The NC Crossroads transition will leverage our proven methodologies and extensive experience in cloud hosting for a seamless and efficient migration. Below is a sampling of clients for whom Voyatek has developed and maintained cloud-hosted solutions:

Client and Project Name	Cloud Provider
North Carolina Child and Adult Care Food Program (CACFP)	Azure Commercial Cloud
South Carolina TeleWIC System	Azure Commercial Cloud
Rhode Island WIC Crossroads	Azure Commercial Cloud
CA Department of Child Support Services – Child Support	Azure Government Cloud
Florida Dept. of Law Enforcement – Florida Incident Based Reporting System and Data Transparency Portal	Azure Government Cloud
Pennsylvania Department of Health – Vital Records	Azure Government Cloud
Connecticut Dept of Emergency Services and Public Protection – Computerized Criminal History MNI	Azure Government Cloud
Montana Community Health Monitoring	AWS
CA Automated Response & Engagement System – Data	AWS
CA Health and Human Services Agency – CAPMAN	AWS

Voyatek's commitment to excellence in cloud hosting and our robust Information Technology Services and Security organization make us the ideal choice for supporting and rehosting the NC WIC Crossroads system.

- ✓ Vision for the Future: The Crossroads smart client architecture is aging and will need modernization in the coming years. Voyatek's development of our next generation of WIC MIS leverages cloud technologies to be more cost-effective for state agencies to operate. Our NextGen architecture will improve participant access and service via greater integration with mobile applications, telehealth systems, external portals, and medical interface partners using a common set of WIC application programming interfaces (APIs). Ease of access and extensibility of system functions are key to improving service for WIC participants. [Voyatek looks forward to sharing our NextGen vision with North Carolina WIC.](#)

Voyatek provides our WIC customers with nutrition subject matter experts, high quality software development, implementation, and cost-effective maintenance support to effectively manage their WIC programs. That commitment has guided us as our WIC business has grown and matured over the last 20 years. Using the most current technology available today, Voyatek is at the forefront of the modernization of WIC technology services, supporting and improving WIC systems that serve millions of participants every day.

[Our proposal highlights Voyatek's WIC experience, stellar staff, and Crossroads system knowledge which provides several unique advantages to benefit North Carolina:](#)

- Zero Learning Curve – No Risk to Ongoing Operations – Voyatek is proposing staff that currently work for North Carolina. Our team’s knowledge and experience avoid the time-consuming process of orienting and adapting to a new M&E contractor, enabling the NC WIC team to continue their focus on providing vital services for North Carolina WIC participants.
- Depth of WIC Resources – Voyatek has over 80 experienced WIC staff that can help resolve issues, support dynamic staffing needs, and provide innovative ideas from their experience on other WIC projects. This depth of resources will enable quick response to North Carolina’s needs for additional enhancements and services.
- Sharing of Knowledge and Ideas from Other WIC Programs – Voyatek supports 25 WIC state agencies (states, territories, and tribal organizations). As we innovate with other WIC programs, we will share those innovations and ideas with North Carolina. What is good for one agency is often good for others. Our track record of doing this for NC WIC demonstrates our commitment to this practice.
- Industry Leader – In support of the WIC mission, Voyatek leaders are involved at the national level working with USDA FNS to provide thought leadership and help shape the future of WIC technology.

North Carolina is looking for a vendor with the best qualifications to maintain and enhance the Crossroads WIC MIS platform. Voyatek’s proposal demonstrates our extensive WIC and Crossroads system knowledge and experience, provides insight into our vision for the future of WIC technology, and highlights the talented team that we have ready to continue working with NC WIC to support the Crossroads system into the future.

a) Signed Execution Page & Solicitation

Voyatek confirms that it has thoroughly reviewed the solicitation document and has provided all requested information as applicable. We affirm our commitment to meeting all requirements and expectations outlined in the solicitation. Please find the signed Execution Page followed by the Solicitation document.

Per the instructions in Ariba 5, Vendor Response, the Signed and Completed Execution Page and a version of the solicitation document has been uploaded in Ariba separately from Voyatek's response document.

Attachment A – Definitions

Attachment A – Definitions is provided on the following pages.

ATTACHMENT A: DEFINITIONS

- 1) **24x7:** A statement of availability of systems, communications, and/or supporting resources every hour (24) of each day (7 days weekly) throughout every year for periods specified herein. Where reasonable downtime is accepted, it will be stated herein. Otherwise, 24x7 implies NO loss of availability of systems, communications, and/or supporting resources.
- 2) **Cybersecurity Incident (GS 143B-1320):** An occurrence that:
 - a. Actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or
 - b. Constitutes a violation or imminent threat of violation of law, security policies, privacy policies, security procedures, or acceptable use policies.
- 3) **Deliverables:** Deliverables, as used herein, shall comprise all Hardware, Vendor Services, professional Services, Software and provided modifications to any Software, and incidental materials, including any goods, Software or Services access license, data, reports and documentation provided or created during the performance or provision of Services hereunder. Deliverables include “Work Product” and means any expression of Licensor’s findings, analyses, conclusions, opinions, recommendations, ideas, techniques, know-how, designs, programs, enhancements, and other technical information; but not source and object code or software.
- 4) **Goods:** Includes intangibles such as computer software; provided, however that this definition does not modify the definition of “goods” in the context of N.C.G.S. §25-2-105 (UCC definition of goods).
- 5) **NCDIT or DIT:** The NC Department of Information Technology.
- 6) **Open Market Contract:** A contract for the purchase of goods or Services not covered by a term, technical, or convenience contract.
- 7) **Reasonable, Necessary or Proper:** as used herein shall be interpreted solely by the State of North Carolina.
- 8) **Request for Proposal (RFP):** The RFP is a formal, written solicitation document typically used for seeking competition and obtaining offers for more complex services or a combination of goods and services. The RFP is used when the value is over \$10,000. This document contains specifications of the RFP, instructions to bidders and the standard IT Terms and Conditions for Goods and Related Services. User should add Supplemental Terms and Conditions for Software and Services, when applicable.
- 9) **Security Breach:** As defined in N.C.G.S. §75-61.
- 10) **Significant Security Incident (GS 143B-1320):** A cybersecurity incident that is likely to result in demonstrable harm to the State's security interests, economy, critical infrastructure, or to the public confidence, civil liberties, or public health and safety of the residents of North Carolina. A significant cybersecurity incident is determined by the following factors:
 - a. Incidents that meet thresholds identified by the Department jointly with the Department of Public Safety that involve information:
 - i. That is not releasable to the public and that is restricted or highly restricted according to Statewide Data Classification and Handling Policy; or
 - ii. That involves the exfiltration, modification, deletion, or unauthorized access, or lack of availability to information or systems within certain parameters to include (i) a specific threshold of number of records or users affected as defined in G.S. 75-65 or (ii) any additional data types with required security controls.

- b. Incidents that involve information that is not recoverable or cannot be recovered within defined time lines required to meet operational commitments defined jointly by the State agency and the Department or can be recovered only through additional measures and has a high or medium functional impact to the mission of an agency.

11) Vendor: Company, firm, corporation, partnership, individual, etc., submitting an offer in response to a solicitation.

12) Additional Defined Terms:

- a. **.NET Framework:** A Microsoft proprietary platform for building desktop, web, and mobile applications.
- b. **ASP.NET:** A server-side web-application framework designed for web development to produce dynamic web pages.
- c. **BFPC:** Breastfeeding Peer Counseling Program, a component of the Crossroads MIS system.
- d. **Central Processing Site:** The data center that hosts Crossroads environments.
- e. **ClickOnce technology:** A deployment technology that enables you to create self-updating Windows-based applications that can be installed and run with minimal user interaction.
- f. **CNSS:** Community Nutrition Services Section, an organization within NC DCFW.
- g. **CR:** Change Request, also known as a Change Order. A design document that describes desired enhancements to the Crossroads MIS system.
- h. **DFDD:** Detailed Functional Design Documents, documentation that defines the detailed business requirements for the Crossroads system.
- i. **DHHS:** The North Carolina Department of Health and Human Services.
- j. **Data Dictionary:** A component of the Detailed Technical Specifications, providing detailed information for each data element in the system.
- k. **Defect:** An error in coding or logic that causes the product to malfunction or to produce incorrect or unexpected results, as required by the DFDD or other regulations and agreements.
- l. **DTS:** Detailed Technical Specifications, documentation that describes various aspects of the system architecture.
- m. **Deployment:** Unless otherwise stipulated, this refers to the phase following completion of UAT, where the Vendor installs the accepted Crossroads release into production.
- n. **Development:** Unless otherwise stipulated, this refers to the phase before UAT, where the Vendor modifies and tests a Crossroads release with agreed maintenance and enhancements.
- o. **Documentation:** Unless otherwise stipulated, this refers to all Crossroads MIS documentation, including but not limited to Detailed Functional Design Documents (DFDD), User Manuals, Detailed Technical Specifications (DTS), Interface Control Documents (ICD), External Communication Documentation (ECD), Report Definition Documentation (RDD), Installation and Configuration Instructions, Central Processing Site Operations Manual, Environment Summary Matrix, Release Notes.
- p. **DCFW:** The Division of Child and Family Well-Being, an organization within NC DHHS.
- q. **EBCI:** Eastern Band of Cherokee Indians, a separate WIC State Agency that utilizes data processing services under the North Carolina Crossroads MIS system.
- r. **EBT:** Electronic Benefit Transfer. This technology allows WIC benefits to be issued and redeemed via magnetically encoded payment cards.
- s. **ECD:** External Communication Documentation, which describes system interfaces to third party systems.
- t. **Environment:** System components, such as servers and databases, on which an instance of the Crossroads software is installed.
- u. **Environment Summary Matrix:** Documentation that summarizes the various versions of software installed on each of the environments.
- v. **FMNP:** Farmers' Market Nutrition Program, a component of the Crossroads MIS system.

- w. **FNS:** Food and Nutrition Service, an agency within the United States Department of Agriculture.
- x. **Handbook 901:** FNS reference and guide for State Agencies that administer WIC programs.
- y. **Hotfix:** A software error correction applied to test or production environments, made quickly and outside of normal development and testing processes. Characterized as a patch, not a release.
- z. **ICD:** Interface Control Document, which describes the system interface to the WIC EBT Provider. Contains far greater detail than an ECD.
- aa. **ISO:** A single software file that contains an exact copy of an optical disk, such as a CD-ROM or DVD.
- bb. **IV&V:** Independent Verification and Validation
- cc. **JAD:** Joint Application Design, a process to collect business requirements.
- dd. **M&E:** Maintenance and Enhancement, the process for ongoing modifications of the Crossroads system after the completion of the initial design, development, and implementation contract.
- ee. **MIS:** Management Information System. The complete Crossroads solution serving WIC state and local offices, WIC retail vendors, WIC participants, and other external stakeholders.
- ff. **Microsoft SQL Server:** A relational database management system (RDBMS) that stores and retrieves data for other software applications
- gg. **Onsite:** All staff are physically present in the subject facilities. No stakeholder is participating via webinar, conference calls, or any other virtual method.
- hh. **RDD:** Report Definition Documentation, which defines data elements and report layouts.
- ii. **Release Notes:** Documentation that describes the details of all software changes, both enhancements and defect corrections, included in a software release.
- jj. **Service Model:** Various levels of computing outsourced to a cloud computing provider, such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS).
- kk. **SSL connection:** Secure Sockets Layer Connection. A communication protocol that creates a secure connection between two devices or applications on a network.
- ll. **Site and System Environment:** The Central Processing Site, and associated infrastructure and platform within the NC Department of Information Technology that hosts the Crossroads system, and the vendor-hosted cloud infrastructure.
- mm. **The State:** Is the State of North Carolina, and its Agencies.
- nn. **Storage Area Network (SAN):** A high-speed network that connects storage devices so that multiple servers and computers can access a shared pool of storage space.
- oo. **Transition-In:** Startup contract activities where the Vendor works with the current incumbent vendor to assume all M&E roles and responsibilities.
- pp. **Transition-Out:** Closeout contract activities where the Vendor transitions its incumbent M&E roles and responsibilities to a new vendor.
- qq. **UAT:** User Acceptance Testing, the phase after Development where the State evaluates the delivered Crossroads release, to determine if it is ready for Deployment.
- rr. **User Manual:** Documentation that describes system operation to end users.
- ss. **Vendor:** Company, firm, corporation, partnership, individual, etc., submitting an offer in response to a solicitation.
- tt. **WBS:** Work Breakdown Structure, a decomposition of the contract into phases, deliverables, and work packages.
- uu. **WIC:** The Supplemental Nutrition Program for Women, Infants, and Children, a federal assistance program provided by FNS.

- vv. **WPF:** The Microsoft technology that runs the Crossroads application on a Windows workstation
- ww. **WUMEI:** WIC Universal MIS-EBT Interface. The design documentation that describes the interface between Crossroads and the EBT Provider.
- xx. **XML-based Web Services:** An industry standard message format used in interfaces between applications.

Attachment B – Department of Information Technology Terms and Conditions for Vendor Hosted Solutions

Attachment B – Department of Information Technology Terms and Conditions for Vendor Hosted Solutions is provided on the following pages.

ATTACHMENT B: DEPARTMENT OF INFORMATION TECHNOLOGY TERMS AND CONDITIONS FOR VENDOR HOSTED SOLUTIONS

Section 1. General Terms and Conditions Applicable to All Purchases

1) **DEFINITIONS:** As used herein;

Agreement means the contract awarded pursuant to this RFP.

Deliverable/Product Warranties shall mean and include the warranties provided for products or deliverables licensed to the State unless superseded by a Vendor's Warranties pursuant to Vendor's License or Support Agreements.

Purchasing State Agency or Agency shall mean the Agency purchasing the goods or Services.

Services shall mean the duties and tasks undertaken by the Vendor to fulfill the requirements and specifications of this solicitation.. Services include, without limitation, providing web browser access by authorized users to Vendor hosted Computer storage, databases, Support, documentation, and other functionalities, all as a Platform as a Service ("PaaS") .

State shall mean the State of North Carolina, the Department of Information Technology (DIT), or the Purchasing State Agency in its capacity as the Contracting Agency, as appropriate.

- 2) **STANDARDS:** Any Deliverables shall meet all applicable State and federal requirements, such as State or Federal Regulation, and NC State Chief Information Officer's (CIO) policy or regulation. Vendor will provide and maintain a quality assurance system or program that includes any Deliverables and will tender or provide to the State only those Deliverables that have been inspected and found to conform to the RFP specifications. All Deliverables are subject to operation, certification, testing and inspection, and any accessibility specifications.
- 3) **WARRANTIES:** Unless otherwise expressly provided, any goods Deliverables provided by the Vendor shall be warranted for a period of 90 days after acceptance.
- 4) **SUBCONTRACTING:** The Vendor may subcontract the performance of required Services with Resources under the Agreement only with the prior written consent of the State contracting authority. Vendor shall provide the State with complete copies of any agreements made by and between Vendor and all subcontractors. The selected Vendor remains solely responsible for the performance of its subcontractors. Subcontractors, if any, shall adhere to the same standards required of the selected Vendor and the Agreement. Any contracts made by the Vendor with a subcontractor shall include an affirmative statement that the State is an intended third party beneficiary of the Agreement; that the subcontractor has no agreement with the State; and that the State shall be indemnified by the Vendor for any claim presented by the subcontractor. Notwithstanding any other term herein, Vendor shall timely exercise its contractual remedies against any non-performing subcontractor and, when appropriate, substitute another subcontractor.
- 5) **TRAVEL EXPENSES:** All travel expenses should be included in the Vendor's proposed costs. Separately stated travel expenses will not be reimbursed. In the event that the Vendor, upon specific request in writing by the State, is deemed eligible to be reimbursed for travel expenses arising under the performance of the Agreement, reimbursement will be at the out-of-state rates set forth in N.C.G.S. §138-6; as amended from time to time. Vendor agrees to use the lowest available airfare not requiring a weekend stay and to use the lowest available rate for rental vehicles. All Vendor incurred travel expenses shall be billed on a monthly basis, shall be supported by receipt and shall be paid by the State within thirty (30) days after invoice approval. Travel expenses exceeding the foregoing rates shall not be paid by the State. The State will reimburse travel allowances only for days on which the Vendor is required to be in North Carolina performing Services under the Agreement.
- 6) **GOVERNMENTAL RESTRICTIONS:** In the event any restrictions are imposed by governmental requirements that necessitate alteration of the material, quality, workmanship, or performance of the Deliverables offered prior to delivery thereof, the Vendor shall provide written notification of the necessary alteration(s) to the Agency Contract Administrator. The State reserves the right to accept any such

alterations, including any price adjustments occasioned thereby, or to cancel the Agreement. The State may advise Vendor of any restrictions or changes in specifications required by North Carolina legislation, rule or regulatory authority that require compliance by the State. In such event, Vendor shall use its best efforts to comply with the required restrictions or changes. If compliance cannot be achieved by the date specified by the State, the State may terminate the Agreement and compensate Vendor for sums then due under the Agreement.

- 7) **PROHIBITION AGAINST CONTINGENT FEES AND GRATUITIES:** Vendor warrants that it has not paid, and agrees not to pay, any bonus, commission, fee, or gratuity to any employee or official of the State for the purpose of obtaining any Contract or award issued by the State. Vendor further warrants that no commission or other payment has been or will be received from or paid to any third party contingent on the award of any Contract by the State, except as shall have been expressly communicated to the State Purchasing Agent in writing prior to acceptance of the Agreement or award in question. Each individual signing below warrants that he or she is duly authorized by their respective Party to sign the Agreement and bind the Party to the terms and conditions of this RFP. Vendor and their authorized signatory further warrant that no officer or employee of the State has any direct or indirect financial or personal beneficial interest, in the subject matter of the Agreement; obligation or Contract for future award of compensation as an inducement or consideration for making the Agreement. Subsequent discovery by the State of non-compliance with these provisions shall constitute sufficient cause for immediate termination of all outstanding contracts. Violations of this provision may result in debarment of the Vendor(s) as permitted by 9 NCAC 06B..1206, or other provision of law.
- 8) **AVAILABILITY OF FUNDS:** Any and all payments to Vendor are expressly contingent upon and subject to the appropriation, allocation and availability of funds to the Agency for the purposes set forth in the Agreement. If the Agreement or any Purchase Order issued hereunder is funded in whole or in part by federal funds, the Agency's performance and payment shall be subject to and contingent upon the continuing availability of said federal funds for the purposes of the Agreement or Purchase Order. If the term of the Agreement extends into fiscal years subsequent to that in which it is approved, such continuation of the Agreement is expressly contingent upon the appropriation, allocation and availability of funds by the N.C. Legislature for the purposes set forth in this RFP. If funds to effect payment are not available, the Agency will provide written notification to Vendor. If the Agreement is terminated under this paragraph, Vendor agrees to take back any affected Deliverables and software not yet delivered under the Agreement, terminate any Services supplied to the Agency under the Agreement, and relieve the Agency of any further obligation thereof. The State shall remit payment for Deliverables and Services accepted prior to the date of the aforesaid notice in conformance with the payment terms.
- 9) **ACCEPTANCE PROCESS:**
- a) The State shall have the obligation to notify Vendor, in writing ten calendar days following provision, performance (under a provided milestone or otherwise as agreed) or delivery of any Services or other Deliverables described in the Agreement that are not acceptable.
 - b) Acceptance testing is required for all Vendor supplied software and software or platform services unless provided otherwise in the solicitation documents or a Statement of Work. The State may define such processes and procedures as may be necessary or proper, in its opinion and discretion, to ensure compliance with the State's specifications, and Vendor's Product Warranties and technical representations. The State shall have the obligation to notify Vendor, in writing and within thirty (30) days following installation of any software deliverable if it is not acceptable.
 - c) Acceptance of Services or other Deliverables including software or platform services may be controlled by an amendment hereto, or additional terms as agreed by the Parties consistent with IT Project management under GS §143B-1340.
 - d) The notice of non-acceptance shall specify in reasonable detail the reason(s) a Service or given Deliverable is unacceptable. Acceptance by the State shall not be unreasonably withheld; but may be conditioned or delayed as required for installation and/or testing of Deliverables. Final acceptance is expressly conditioned upon completion of any applicable inspection and testing procedures. Should a Service or Deliverable fail to meet any specifications or acceptance criteria, the State may exercise any and all rights hereunder. Services or Deliverables discovered to be defective or failing to conform

to the specifications may be rejected upon initial inspection or at any later time if the defects or errors contained in the Services or Deliverables or non-compliance with the specifications were not reasonably ascertainable upon initial inspection. If the Vendor fails to promptly cure or correct the defect or replace or re-perform the Services or Deliverables, the State reserves the right to cancel the Purchase Order, contract with a different Vendor, and to invoice the original Vendor for any differential in price over the original Contract price.

- 10) PAYMENT TERMS:** Monthly Payment terms are Net 30 days after receipt of correct invoice and acceptance of one or more of the Deliverables, under milestones or otherwise as may be provided in Paragraph 9 (Acceptance), or elsewhere in this solicitation, unless a period of more than thirty (30) days is required by the Agency. The Purchasing State Agency is responsible for all payments under the Agreement. No additional charges to the Agency will be permitted based upon, or arising from, the Agency's use of a Business Procurement Card. The State may exercise any and all rights of Set Off as permitted in Chapter 105A-1 *et. seq.* of the N.C. General Statutes and applicable Administrative Rules. Upon Vendor's written request of not less than thirty (30) days and approval by the State or Agency, the Agency may:
- a) Forward the Vendor's payment check(s) directly to any person or entity designated by the Vendor, or
 - b) Include any person or entity designated in writing by Vendor as a joint payee on the Vendor's payment check(s), however
 - c) In no event shall such approval and action obligate the State to anyone other than the Vendor and the Vendor shall remain responsible for fulfillment of all Contract obligations.
- 11) EQUAL EMPLOYMENT OPPORTUNITY:** Vendor shall comply with all Federal and State requirements concerning fair employment and employment of the disabled, and concerning the treatment of all employees without regard to discrimination by reason of race, color, religion, sex, national origin or physical disability.
- 12) ADVERTISING/PRESS RELEASE:** The Vendor absolutely shall not publicly disseminate any information concerning the Agreement without prior written approval from the State or its Agent. For the purpose of this provision of the Agreement, the Agent is the Purchasing Agency Contract Administrator unless otherwise named in the solicitation documents.
- 13) LATE DELIVERY:** Vendor shall advise the Agency contact person or office immediately upon determining that any Deliverable will not, or may not, be delivered or performed at the time or place specified. Together with such notice, Vendor shall state the projected delivery time and date. In the event the delay projected by Vendor is unsatisfactory, the Agency shall so advise Vendor and may proceed to procure the particular substitute Services or other Deliverables.
- 14) ACCESS TO PERSONS AND RECORDS:** Pursuant to N.C.G.S. §147-64.7, the Agency, the State Auditor, appropriate federal officials, and their respective authorized employees or agents are authorized to examine all books, records, and accounts of the Vendor insofar as they relate to transactions with any department, board, officer, commission, institution, or other agency of the State of North Carolina pursuant to the performance of the Agreement or to costs charged to the Agreement. The Vendor shall retain any such books, records, and accounts for a minimum of three (3) years after the completion of the Agreement. Additional audit or reporting requirements may be required by any Agency, if in the Agency's opinion, such requirement is imposed by federal or state law or regulation.
- 15) ASSIGNMENT:** Vendor may not assign the Agreement or its obligations hereunder except as permitted by 09 NCAC 06B.1003 and this Paragraph. Vendor shall provide reasonable notice of not less than thirty (30) days prior to any consolidation, acquisition, or merger. Any assignee shall affirm the Agreement attorning and agreeing to the terms and conditions agreed, and that Vendor shall affirm that the assignee is fully capable of performing all obligations of Vendor under the Agreement. An assignment may be made, if at all, in writing by the Vendor, Assignee and the State setting forth the foregoing obligation of Vendor and Assignee.
- 16) INSURANCE COVERAGE:** During the term of the Agreement, the Vendor at its sole cost and expense shall provide commercial insurance of such type and with such terms and limits as may be reasonably associated with the Agreement. As a minimum, the Vendor shall provide and maintain the following coverage and limits:

- a) **Worker's Compensation** - The Vendor shall provide and maintain Worker's Compensation Insurance, as required by the laws of North Carolina, as well as employer's liability coverage with minimum limits of \$100,000.00, covering all of Vendor's employees who are engaged in any work under the Agreement. If any work is sublet, the Vendor shall require the subcontractor to provide the same coverage for any of his employees engaged in any work under the Agreement; and
- b) **Commercial General Liability** - General Liability Coverage on a Comprehensive Broad Form on an occurrence basis in the minimum amount of \$2,000,000.00 Combined Single Limit (Defense cost shall be in excess of the limit of liability); and
- c) **Automobile** - Automobile Liability Insurance, to include liability coverage, covering all owned, hired and non-owned vehicles, used in connection with the Agreement. The minimum combined single limit shall be \$500,000.00 bodily injury and property damage; \$500,000.00 uninsured/under insured motorist; and \$5,000.00 medical payment; and
- d) Providing and maintaining adequate insurance coverage described herein is a material obligation of the Vendor and is of the essence of the Agreement. All such insurance shall meet all laws of the State of North Carolina. Such insurance coverage shall be obtained from companies that are authorized to provide such coverage and that are authorized by the Commissioner of Insurance to do business in North Carolina. The Vendor shall at all times comply with the terms of such insurance policies, and all requirements of the insurer under any such insurance policies, except as they may conflict with existing North Carolina laws or the Agreement. The limits of coverage under each insurance policy maintained by the Vendor shall not be interpreted as limiting the Vendor's liability and obligations under the Agreement.

17) DISPUTE RESOLUTION: The parties agree that it is in their mutual interest to resolve disputes informally. A claim by the Vendor shall be submitted in writing to the Agency Contract Administrator for decision. A claim by the State shall be submitted in writing to the Vendor's Contract Administrator for decision. The Parties shall negotiate in good faith and use all reasonable efforts to resolve such dispute(s). During the time the Parties are attempting to resolve any dispute, each shall proceed diligently to perform their respective duties and responsibilities under the Agreement. If a dispute cannot be resolved between the Parties within thirty (30) days after delivery of notice, either Party may elect to exercise any other remedies available under the Agreement, or at law. This term shall not constitute an agreement by either party to mediate or arbitrate any dispute.

18) CONFIDENTIALITY: In accordance with N.C.G.S. §143B-1350(e) and 143B-1375, and 09 NCAC 06B.0103 and 06B.1001, the State may maintain the confidentiality of certain types of information described in N.C.G.S. §132-1 *et seq.* Such information may include trade secrets defined by N.C.G.S. §66-152 and other information exempted from the Public Records Act pursuant to N.C.G.S. §132-1.2. Vendor may designate appropriate portions of its response as confidential, consistent with and to the extent permitted under the Statutes and Rules set forth above, by marking the top and bottom of pages containing confidential information with a legend in boldface type "**CONFIDENTIAL**". By so marking any page, the Vendor warrants that it has formed a good faith opinion, having received such necessary or proper review by counsel and other knowledgeable advisors that the portions marked confidential meet the requirements of the Rules and Statutes set forth above. ***However, under no circumstances shall price information be designated as confidential.*** The State may serve as custodian of Vendor's confidential information and not as an arbiter of claims against Vendor's assertion of confidentiality. If an action is brought pursuant to N.C.G.S. §132-9 to compel the State to disclose information marked confidential, the Vendor agrees that it will intervene in the action through its counsel and participate in defending the State, including any public official(s) or public employee(s). The Vendor agrees that it shall hold the State and any official(s) and individual(s) harmless from any and all damages, costs, and attorneys' fees awarded against the State in the action. The State agrees to promptly notify the Vendor in writing of any action seeking to compel the disclosure of Vendor's confidential information. The State shall have the right, at its option and expense, to participate in the defense of the action through its counsel. The State shall have no liability to Vendor with respect to the disclosure of Vendor's confidential information ordered by a court of competent jurisdiction pursuant to N.C.G.S. §132-9 or other applicable law.

- a) Care of Information: Vendor agrees to use commercial best efforts to safeguard and protect any data, documents, files, and other materials received from the State or the Agency during performance of any contractual obligation from loss, destruction or erasure. Vendor agrees to abide by all facilities and security requirements and policies of the agency where work is to be performed. Any Vendor personnel shall abide by such facilities and security requirements and shall agree to be bound by the terms and conditions of the Agreement.
- b) Vendor warrants that all its employees and any approved third party Vendors or subcontractors are subject to a non-disclosure and confidentiality agreement enforceable in North Carolina. Vendor will, upon request of the State, verify and produce true copies of any such agreements. Production of such agreements by Vendor may be made subject to applicable confidentiality, non-disclosure or privacy laws; provided that Vendor produces satisfactory evidence supporting exclusion of such agreements from disclosure under the N.C. Public Records laws in N.C.G.S. §132-1 *et seq.* The State may, in its sole discretion, provide a non-disclosure and confidentiality agreement satisfactory to the State for Vendor's execution. The State may exercise its rights under this subparagraph as necessary or proper, in its discretion, to comply with applicable security regulations or statutes including, but not limited to 26 USC 6103 and IRS Publication 1075, (Tax Information Security Guidelines for Federal, State, and Local Agencies), HIPAA, 42 USC 1320(d) (Health Insurance Portability and Accountability Act), any implementing regulations in the Code of Federal Regulations, and any future regulations imposed upon the Department of Information Technology or the N.C. Department of Revenue pursuant to future statutory or regulatory requirements.
- c) Nondisclosure: Vendor agrees and specifically warrants that it, its officers, directors, principals and employees, and any subcontractors, shall hold all information received during performance of the Agreement in the strictest confidence and shall not disclose the same to any third party without the express written approval of the State.
- d) The Vendor shall protect the confidentiality of all information, data, instruments, studies, reports, records and other materials provided to it by the Agency or maintained or created in accordance with this Agreement. No such information, data, instruments, studies, reports, records and other materials in the possession of Vendor shall be disclosed in any form without the prior written consent of the State Agency. The Vendor will have written policies governing access to and duplication and dissemination of all such information, data, instruments, studies, reports, records and other materials.
- e) All project materials, including software, data, and documentation created during the performance or provision of Services hereunder that are not licensed to the State or are not proprietary to the Vendor are the property of the State of North Carolina and must be kept confidential or returned to the State, or destroyed. Proprietary Vendor materials shall be identified to the State by Vendor prior to use or provision of Services hereunder and shall remain the property of the Vendor. Derivative works of any Vendor proprietary materials prepared or created during the performance of provision of Services hereunder shall be subject to a perpetual, royalty free, nonexclusive license to the State.

19) DEFAULT: In the event Services or other Deliverable furnished or performed by the Vendor during performance of any Contract term fail to conform to any material requirement(s) of the Contract specifications, notice of the failure is provided by the State and if the failure is not cured within ten (10) days, or Vendor fails to meet the requirements of Paragraph 9) herein, the State may cancel the contract. Default may be cause for debarment as provided in 09 NCAC 06B.1206. The rights and remedies of the State provided above shall not be exclusive and are in addition to any other rights and remedies provided by law or under the Contract.

- a) If Vendor fails to deliver or provide correct Services or other Deliverables within the time required by the Agreement, the State shall provide written notice of said failure to Vendor, and by such notice require performance assurance measures pursuant to N.C.G.S. 143B-1340(f). Vendor is responsible for the delays resulting from its failure to deliver or provide services or other Deliverables.
- b) Should the State fail to perform any of its obligations upon which Vendor's performance is conditioned, Vendor shall not be in default for any delay, cost increase or other consequences resulting from the State's failure. Vendor will use reasonable efforts to mitigate delays, costs or expenses arising from assumptions in the Vendor's offer documents that prove erroneous or are

otherwise invalid. Any deadline that is affected by any such failure in assumptions or performance by the State shall be extended by an amount of time reasonably necessary to compensate for the effect of such failure.

- c) Vendor shall provide a plan to cure any delay or default if requested by the State. The plan shall state the nature of the delay or default, the time required for cure, any mitigating factors causing or tending to cause the delay or default, and such other information as the Vendor may deem necessary or proper to provide.
- d) If the prescribed acceptance testing stated in the Solicitation Documents or performed pursuant to Paragraph 9) of the DIT Terms and Conditions is not completed successfully, the State may request substitute Software, cancel the portion of the Contract that relates to the unaccepted Software, or continue the acceptance testing with or without the assistance of Vendor. These options shall remain in effect until such time as the testing is successful or the expiration of any time specified for completion of the testing. If the testing is not completed after exercise of any of the State's options, the State may cancel any portion of the contract related to the failed Software and take action to procure substitute software. If the failed software (or the substituted software) is an integral and critical part of the proper completion of the work for which the Deliverables identified in the solicitation documents or statement of work were acquired, the State may terminate the entire contract.

20) WAIVER OF DEFAULT: Waiver by either party of any default or breach by the other Party shall not be deemed a waiver of any subsequent default or breach and shall not be construed to be a modification or novation of the terms of the Agreement, unless so stated in writing and signed by authorized representatives of the Agency and the Vendor, and made as an amendment to the Agreement pursuant to Paragraph 40) herein below.

21) TERMINATION: Any notice or termination made under the Agreement shall be transmitted via US Mail, Certified Return Receipt Requested. The period of notice for termination shall begin on the day the return receipt is signed and dated.

- a) The parties may mutually terminate the Agreement by written agreement at any time.
- b) The State may terminate the Agreement, in whole or in part, pursuant to Paragraph 19), or pursuant to the Special Terms and Conditions in the Solicitation Documents, if any, or for any of the following:
 - i) Termination for Cause: In the event any goods, software, or service furnished by the Vendor during performance of any Contract term fails to conform to any material requirement of the Contract, and the failure is not cured within the specified time after providing written notice thereof to Vendor, the State may cancel and procure the articles or Services from other sources; holding Vendor liable for any excess costs occasioned thereby, subject only to the limitations provided in Paragraphs 22) and 23) herein. The rights and remedies of the State provided above shall not be exclusive and are in addition to any other rights and remedies provided by law or under the Contract. Vendor shall not be relieved of liability to the State for damages sustained by the State arising from Vendor's breach of the Agreement; and the State may, in its discretion, withhold any payment due as a setoff until such time as the damages are finally determined or as agreed by the parties. Voluntary or involuntary Bankruptcy or receivership by Vendor shall be cause for termination.
 - ii) Termination For Convenience Without Cause: The State may terminate service and indefinite quantity contracts, in whole or in part by giving thirty (30) days prior notice in writing to the Vendor. Vendor shall be entitled to sums due as compensation for Deliverables provided and Services performed in conformance with the Contract. In the event the Contract is terminated for the convenience of the State the Agency will pay for all work performed and products delivered in conformance with the Contract up to the date of termination.
 - iii) Consistent failure to participate in problem resolution meetings, two (2) consecutive missed or rescheduled meetings, or failure to make a good faith effort to resolve problems, may result in termination of the Agreement.

22) LIMITATION OF VENDOR'S LIABILITY:

- a) Where Deliverables are under the State's exclusive management and control, the Vendor shall not be liable for direct damages caused by the State's failure to fulfill any State responsibilities of assuring the

proper use, management and supervision of the Deliverables and programs, audit controls, operating methods, office procedures, or for establishing all proper checkpoints necessary for the State's intended use of the Deliverables. Vendor shall not be responsible for any damages that arise from (i) misuse or modification of Vendor's Software by or on behalf of the State, (ii) the State's failure to use corrections or enhancements made available by Vendor, (iii) the quality or integrity of data from other automated or manual systems with which the Vendor's Software interfaces, (iv) errors in or changes to third party software or hardware implemented by the State or a third party (including the vendors of such software or hardware) that is not a subcontractor of Vendor or that is not supported by the Deliverables, or (vi) the operation or use of the Vendor's Software not in accordance with the operating procedures developed for the Vendor's Software or otherwise in a manner not contemplated by this Agreement.

- b) The Vendor's liability for damages to the State arising under the contract shall be limited to two times the value of the Contract.
- c) The foregoing limitation of liability shall not apply to claims covered by other specific provisions including but not limited to Service Level Agreement or Deliverable/Product Warranties pursuant to Section II, 2) of these Terms and Conditions, or to claims for injury to persons or damage to tangible personal property, gross negligence or willful or wanton conduct. This limitation of liability does not apply to contributions among joint tortfeasors under N.C.G.S. 1B-1 *et seq.*, the receipt of court costs or attorney's fees that might be awarded by a court in addition to damages after litigation based on the Agreement. For avoidance of doubt, the Parties agree that the Service Level Agreement and Deliverable/Product Warranty Terms in the Contract are intended to provide the sole and exclusive remedies available to the State under the Contract for the Vendor's failure to comply with the requirements stated therein.

23) VENDOR'S LIABILITY FOR INJURY TO PERSONS OR DAMAGE TO PROPERTY:

- a) The Vendor shall be liable for damages arising out of personal injuries and/or damage to real or tangible personal property of the State, employees of the State, persons designated by the State for training, or person(s) other than agents or employees of the Vendor, designated by the State for any purpose, prior to, during, or subsequent to delivery, installation, acceptance, and use of the Deliverables either at the Vendor's site or at the State's place of business, provided that the injury or damage was caused by the fault or negligence of the Vendor.
- b) The Vendor agrees to indemnify, defend and hold the Agency and the State and its Officers, employees, agents and assigns harmless from any liability relating to personal injury or injury to real or personal property of any kind, accruing or resulting to any other person, firm or corporation furnishing or supplying work, Services, materials or supplies in connection with the performance of the Agreement, whether tangible or intangible, arising out of the ordinary negligence, wilful or wanton negligence, or intentional acts of the Vendor, its officers, employees, agents, assigns or subcontractors.
- c) Vendor shall not be liable for damages arising out of or caused by an alteration or an attachment not made or installed by the Vendor.

24) TIME IS OF THE ESSENCE: Time is of the essence in the performance of the Agreement.

25) DATE AND TIME WARRANTY: The Vendor warrants that any Deliverable, whether Services, hardware, firmware, middleware, custom or commercial software, or internal components, subroutines, and interface therein which performs, modifies or affects any date and/or time data recognition function, calculation, or sequencing, will still enable the modified function to perform accurate date/time data and leap year calculations. This warranty shall survive termination or expiration of the Contract.

26) INDEPENDENT CONTRACTORS: Vendor and its employees, officers and executives, and subcontractors, if any, shall be independent Vendors and not employees or agents of the State. The Agreement shall not operate as a joint venture, partnership, trust, agency or any other similar business relationship.

27) TRANSPORTATION: Transportation of any tangible Deliverables shall be FOB Destination; unless otherwise specified in the solicitation document or purchase order. Freight, handling, hazardous material charges, and distribution and installation charges shall be included in the total price of each item. Any

additional charges shall not be honored for payment unless authorized in writing by the Purchasing State Agency. In cases where parties, other than the Vendor ship materials against this order, the shipper must be instructed to show the purchase order number on all packages and shipping manifests to ensure proper identification and payment of invoices. A complete packing list must accompany each shipment.

28) NOTICES: Any notices required under the Agreement should be delivered to the Contract Administrator for each party. Unless otherwise specified in the Solicitation Documents, any notices shall be delivered in writing by U.S. Mail, Commercial Courier or by hand.

29) TITLES AND HEADINGS: Titles and Headings in the Agreement are used for convenience only and do not define, limit or proscribe the language of terms identified by such Titles and Headings.

30) AMENDMENT: The Agreement may not be amended orally or by performance. Any amendment must be made in written form and signed by duly authorized representatives of the State and Vendor in conformance with Paragraph 36) herein.

31) TAXES: The State of North Carolina is exempt from Federal excise taxes and no payment will be made for any personal property taxes levied on the Vendor or for any taxes levied on employee wages. Agencies of the State may have additional exemptions or exclusions for federal or state taxes. Evidence of such additional exemptions or exclusions may be provided to Vendor by Agencies, as applicable, during the term of the Agreement. Applicable State or local sales taxes shall be invoiced as a separate item.

32) GOVERNING LAWS, JURISDICTION, AND VENUE:

a) The Agreement is made under and shall be governed and construed in accordance with the laws of the State of North Carolina and applicable Administrative Rules. The place of the Agreement or purchase order, its situs and forum, shall be Wake County, North Carolina, where all matters, whether sounding in Contract or in tort, relating to its validity, construction, interpretation and enforcement shall be determined. Vendor agrees and submits, solely for matters relating to the Agreement, to the jurisdiction of the courts of the State of North Carolina, and stipulates that Wake County shall be the proper venue for all matters.

b) Except to the extent the provisions of the Contract are clearly inconsistent therewith, the applicable provisions of the Uniform Commercial Code as modified and adopted in North Carolina shall govern the Agreement. To the extent the Contract entails both the supply of "goods" and "Services," such shall be deemed "goods" within the meaning of the Uniform Commercial Code, except when deeming such Services as "goods" would result in a clearly unreasonable interpretation.

33) FORCE MAJEURE: Neither party shall be deemed to be in default of its obligations hereunder if and so long as it is prevented from performing such obligations as a result of events beyond its reasonable control, including without limitation, fire, power failures, any act of war, hostile foreign action, nuclear explosion, riot, strikes or failures or refusals to perform under subcontracts, civil insurrection, earthquake, hurricane, tornado, or other catastrophic natural event or act of God.

34) COMPLIANCE WITH LAWS: The Vendor shall comply with all laws, ordinances, codes, rules, regulations, and licensing requirements that are applicable to the conduct of its business, including those of federal, state, and local agencies having jurisdiction and/or authority.

35) SEVERABILITY: In the event that a court of competent jurisdiction holds that a provision or requirement of the Agreement violates any applicable law, each such provision or requirement shall be enforced only to the extent it is not in violation of law or is not otherwise unenforceable and all other provisions and requirements of the Agreement shall remain in full force and effect. All promises, requirement, terms, conditions, provisions, representations, guarantees and warranties contained herein shall survive the expiration or termination date unless specifically provided otherwise herein, or unless superseded by applicable federal or State statute, including statutes of repose or limitation.

36) CHANGES: The Agreement and subsequent purchase order(s) is awarded subject to the provision of the specified Services and the shipment or provision of other Deliverables as specified herein. Any changes made to the Agreement or purchase order proposed by the Vendor are hereby rejected unless accepted in writing by the Agency or State Award Authority. The State shall not be responsible for Services or other Deliverables delivered without a purchase order from the Agency or State Award Authority.

37) FEDERAL INTELLECTUAL PROPERTY BANKRUPTCY PROTECTION ACT: The Parties agree that the Agency shall be entitled to all rights and benefits of the Federal Intellectual Property Bankruptcy Protection Act, Public Law 100-506, codified at 11 U.S.C. 365(n), and any amendments thereto.

38) ELECTRONIC PROCUREMENT (Applies to all contracts that include E-Procurement and are identified as such in the body of the solicitation document): Purchasing shall be conducted through the Statewide E-Procurement Services. The State's third party agent shall serve as the Supplier Manager for this E-Procurement Services. The Vendor shall register for the Statewide E-Procurement Services within two (2) business days of notification of award in order to receive an electronic purchase order resulting from award of the Agreement.

- a) **The successful Vendor(s) shall pay a transaction fee of 1.75% (.0175) on the total dollar amount (excluding sales taxes) of each purchase order issued through the Statewide E-Procurement Service.** This applies to all purchase orders, regardless of the quantity or dollar amount of the purchase order. The transaction fee shall neither be charged to nor paid by the State, or by any State approved users of the contract. The transaction fee shall not be stated or included as a separate item in the proposed contract or invoice. There are no additional fees or charges to the Vendor for the Services rendered by the Supplier Manager under the Agreement. Vendor will receive a credit for transaction fees they paid for the purchase of any item(s) if an item(s) is returned through no fault of the Vendor. Transaction fees are non-refundable when an item is rejected and returned, or declined, due to the Vendor's failure to perform or comply with specifications or requirements of the contract.
- b) Vendor, or its authorized Reseller, as applicable, will be invoiced monthly for the State's transaction fee by the Supplier Manager. The transaction fee shall be based on purchase orders issued for the prior month. Unless Supplier Manager receives written notice from the Vendor identifying with specificity any errors in an invoice within thirty (30) days of the receipt of invoice, such invoice shall be deemed to be correct and Vendor shall have waived its right to later dispute the accuracy and completeness of the invoice. Payment of the transaction fee by the Vendor is due to the account designated by the State within thirty (30) days after receipt of the correct invoice for the transaction fee, which includes payment of all portions of an invoice not in dispute. Within thirty (30) days of the receipt of invoice, Vendor may request in writing an extension of the invoice payment due date for that portion of the transaction fee invoice for which payment of the related goods by the governmental purchasing entity has not been received by the Vendor. If payment of the transaction fee invoice is not received by the State within this payment period, it shall be considered a material breach of contract. The Supplier Manager shall provide, whenever reasonably requested by the Vendor in writing (including electronic documents), supporting documentation from the E-Procurement Service that accounts for the amount of the invoice.
- c) The Supplier Manager will capture the order from the State approved user, including the shipping and payment information, and submit the order in accordance with the E-Procurement Services. Subsequently, the Supplier Manager will send those orders to the appropriate Vendor on State Contract. The State or State approved user, not the Supplier Manager, shall be responsible for the solicitation, offers received, evaluation of offers received, award of Contract, and the payment for goods delivered.
- d) Vendor agrees at all times to maintain the confidentiality of its user name and password for the Statewide E-Procurement Services. If a Vendor is a corporation, partnership or other legal entity, then the Vendor may authorize its employees to use its password. Vendor shall be responsible for all activity and all charges for such employees. Vendor agrees not to permit a third party to use the Statewide E-Procurement Services through its account. If there is a breach of security through the Vendor's account, Vendor shall immediately change its password and notify the Supplier Manager of the security breach by e-mail. Vendor shall cooperate with the state and the Supplier Manager to mitigate and correct any security breach.
- e) The transaction fee applies only to commodities obtained under this contract, if any. The transaction fee does not apply to services obtained under this contract.

39) PATENT, COPYRIGHT, AND TRADE SECRET PROTECTION:

- a) Vendor has created, acquired or otherwise has rights in, and may, in connection with the performance of Services for the State, employ, provide, create, acquire or otherwise obtain rights in various concepts, ideas, methods, methodologies, procedures, processes, know-how, techniques, models, templates and general purpose consulting and software tools, utilities and routines (collectively, the "Vendor technology"). To the extent that any Vendor technology is contained in any of the Services or Deliverables including any derivative works, the Vendor hereby grants the State a royalty-free, fully paid, worldwide, perpetual, non-exclusive license to use such Vendor technology in connection with the Services or Deliverables for the State's purposes.
- b) Vendor shall not acquire any right, title and interest in and to the copyrights for goods, any and all software, technical information, specifications, drawings, records, documentation, data or derivative works thereof, or other work products provided by the State to Vendor. The State hereby grants Vendor a royalty-free, fully paid, worldwide, perpetual, non-exclusive license for Vendor's internal use to non-confidential deliverables first originated and prepared by the Vendor for delivery to the State.
- c) The Vendor, at its own expense, shall defend any action brought against the State to the extent that such action is based upon a claim that the Services or other Deliverables supplied by the Vendor, or the operation of such pursuant to a current version of vendor-supplied software, infringes a patent, or copyright or violates a trade secret in the United States. The Vendor shall pay those costs and damages finally awarded against the State in any such action; damages shall be limited as provided in N.C.G.S. 143B-1350(h1). Such defense and payment shall be conditioned on the following:
 - i. That the Vendor shall be notified within a reasonable time in writing by the State of any such claim; and,
 - ii. That the Vendor shall have the sole control of the defense of any action on such claim and all negotiations for its settlement or compromise, provided, however, that the State shall have the option to participate in such action at its own expense.
- d) Should any Services or other Deliverables supplied by Vendor, or the operation thereof become, or in the Vendor's opinion are likely to become, the subject of a claim of infringement of a patent, copyright, or a trade secret in the United States, the State shall permit the Vendor, at its option and expense, either to procure for the State the right to continue using the Services or Deliverables, or to replace or modify the same to become noninfringing and continue to meet procurement specifications in all material respects. If neither of these options can reasonably be taken, or if the use of such Services or Deliverables by the State shall be prevented by injunction, the Vendor agrees to take back any goods/hardware or software, and refund any sums the State has paid Vendor less any reasonable amount for use or damage and make every reasonable effort to assist the state in procuring substitute Services or Deliverables. If, in the sole opinion of the State, the return of such infringing Services or Deliverables makes the retention of other Services or Deliverables acquired from the Vendor under the agreement impractical, the State shall then have the option of terminating the contract, or applicable portions thereof, without penalty or termination charge. The Vendor agrees to take back Services or Deliverables and refund any sums the State has paid Vendor less any reasonable amount for use or damage.
- e) Vendor will not be required to defend or indemnify the State if any claim by a third party against the State for infringement or misappropriation (i) results from the State's alteration of any Vendor-branded Service or Deliverable, or (ii) results from the continued use of the good(s) or services and other Services or Deliverables after receiving notice they infringe a trade secret of a third party.
- f) Nothing stated herein, however, shall affect Vendor's ownership in or rights to its preexisting intellectual property and proprietary rights.

40) UNANTICIPATED TASKS In the event that additional work must be performed that was wholly unanticipated, and that is not specified in the Agreement, but which in the opinion of both parties is necessary to the successful accomplishment of the contracted scope of work, the procedures outlined in this article will be followed. For each item of unanticipated work, the Vendor shall prepare a work authorization in accordance with the State's practices and procedures.

- a) It is understood and agreed by both parties that all of the terms and conditions of the Agreement shall remain in force with the inclusion of any work authorization. A work authorization shall not constitute a contract separate from the Agreement, nor in any manner amend or supersede any of the other terms or provisions of the Agreement or any amendment hereto.
- b) Each work authorization shall comprise a detailed statement of the purpose, objective, or goals to be undertaken by the Vendor, the job classification or approximate skill level or sets of the personnel required, an identification of all significant material then known to be developed by the Vendor's personnel as a Deliverable, an identification of all significant materials to be delivered by the State to the Vendor's personnel, an estimated time schedule for the provision of the Services by the Vendor, completion criteria for the work to be performed, the name or identification of Vendor's personnel to be assigned, the Vendor's estimated work hours required to accomplish the purpose, objective or goals, the Vendor's billing rates and units billed, and the Vendor's total estimated cost of the work authorization.
- c) All work authorizations must be submitted for review and approval by the procurement office that approved the original Contract and procurement. This submission and approval must be completed prior to execution of any work authorization documentation or performance thereunder. All work authorizations must be written and signed by the Vendor and the State prior to beginning work.
- d) The State has the right to require the Vendor to stop or suspend performance under the "Stop Work" provision of the North Carolina Department of Information Technology Terms and Conditions.
- e) The Vendor shall not expend Personnel resources at any cost to the State in excess of the estimated work hours unless this procedure is followed: If, during performance of the work, the Vendor determines that a work authorization to be performed under the Agreement cannot be accomplished within the estimated work hours, the Vendor will be required to complete the work authorization in full. Upon receipt of such notification, the State may:
 - a. Authorize the Vendor to expend the estimated additional work hours or service in excess of the original estimate necessary to accomplish the work authorization, or
 - b. Terminate the work authorization, or
 - c. Alter the scope of the work authorization in order to define tasks that can be accomplished within the remaining estimated work hours.
 - d. The State will notify the Vendor in writing of its election within seven (7) calendar days after receipt of the Vendor's notification. If notice of the election is given to proceed, the Vendor may expend the estimated additional work hours or Services.

41) STOP WORK ORDER The State may issue a written Stop Work Order to Vendor for cause at any time requiring Vendor to suspend or stop all, or any part, of the performance due under the Agreement for a period up to ninety (90) days after the Stop Work Order is delivered to the Vendor. The ninety (90) day period may be extended for any further period for which the parties may agree.

- a) The Stop Work Order shall be specifically identified as such and shall indicate that it is issued under this term. Upon receipt of the Stop Work Order, the Vendor shall immediately comply with its terms and take all reasonable steps to minimize incurring costs allocable to the work covered by the Stop Work Order during the period of work suspension or stoppage. Within a period of ninety (90) days after a Stop Work Order is delivered to Vendor, or within any extension of that period to which the parties agree, the State shall either:
 - i) Cancel the Stop Work Order, or
 - ii) Terminate the work covered by the Stop Work Order as provided for in the termination for default or the termination for convenience clause of the Agreement.

- b) If a Stop Work Order issued under this clause is canceled or the period of the Stop Work Order or any extension thereof expires, the Vendor shall resume work. The State shall make an equitable adjustment in the delivery schedule, the Agreement price, or both, and the Agreement shall be modified, in writing, accordingly, if:
 - i) The Stop Work Order results in an increase in the time required for, or in the Vendor's cost properly allocable to the performance of any part of the Agreement, and
 - ii) The Vendor asserts its right to an equitable adjustment within thirty (30) days after the end of the period of work stoppage; provided that if the State decides the facts justify the action, the State may receive and act upon an offer submitted at any time before final payment under the Agreement.
- c) If a Stop Work Order is not canceled and the work covered by the Stop Work Order is terminated in accordance with the provision entitled Termination for Convenience of the State, the State shall allow reasonable direct costs resulting from the Stop Work Order in arriving at the termination settlement.
- d) The State shall not be liable to the Vendor for loss of profits because of a Stop Work Order issued under this term.

41) TRANSITION ASSISTANCE If the Agreement is not renewed at the end of the term, or is canceled prior to its expiration, for any reason, the Vendor must provide for up to six (6) months after the expiration or cancellation of the Agreement, all reasonable transition assistance requested by the State, to allow for the expired or canceled portion of the Services to continue without interruption or adverse effect, and to facilitate the orderly transfer of such Services to the State or its designees. Such transition assistance will be deemed by the parties to be governed by the terms and conditions of the Agreement, (notwithstanding this expiration or cancellation) except for those Contract terms or conditions that do not reasonably apply to such transition assistance. The State shall pay the Vendor for any resources utilized in performing such transition assistance at the most current rates provided by the Agreement for Contract performance. If the State cancels the Agreement for cause, then the State will be entitled to off set the cost of paying the Vendor for the additional resources the Vendor utilized in providing transition assistance with any damages the State may have otherwise accrued as a result of said cancellation.

42) STATE PROPERTY AND INTANGIBLES RIGHTS: The parties acknowledge and agree that the State shall own all right, title and interest in and to the copyright in any and all software, technical information, specifications, drawings, records, documentation, data and other work products first originated and prepared by the Vendor for delivery to the State (the "Deliverables"). To the extent that any Vendor Technology is contained in any of the Deliverables, the Vendor hereby grants the State a royalty-free, fully paid, worldwide, perpetual, non-exclusive license to use such Vendor Technology in connection with the Deliverables for the State's internal business purposes. Vendor shall not acquire any right, title and interest in and to the copyrights for goods, any and all software, technical information, specifications, drawings, records, documentation, data or derivative works thereof, or other work products provided by the State to Vendor. The State hereby grants Vendor a royalty-free, fully paid, worldwide, perpetual, non-exclusive license to non-confidential Deliverables first originated and prepared by the Vendor for delivery to the State.

Section 2: Terms and Conditions Applicable to Vendor Hosted Services (e.g., Platform as a Service ("PaaS"); Infrastructure as a Service ("IaaS"))

1) DEFINITIONS:

- a) "Data" includes all materials provided by the State to the Vendor, including but not limited to software, technical information, specifications, drawings, records, and documentation, as well as includes and means the information, formulae, algorithms, or other content that the State, the State's employees, agents and end users upload, create or modify using the Services pursuant to this Agreement. Data

also includes user identification information and metadata which may contain Data or from which the State's Data may be ascertainable.

- b) "Support" includes provision of ongoing updates and maintenance for the Vendor online software applications, and as may be specified herein, consulting, training and other support Services as provided by the Vendor to meet the requirements and specifications of this RFP and for Vendor's tenants receiving similar Services.

2) **ACCESS AND USE OF VENDOR HOSTED SERVICES:**

- a) The Vendor grants the State a personal non-transferable and non-exclusive right to use and access, all Services and other functionalities or services provided, furnished or accessible under this Agreement. The State is authorized to access the State's Data and any Vendor-provided data as specified herein and to transmit revisions, updates, deletions, enhancements, or modifications to the State Data. The State may use the Services with any computer, computer system, server, or desktop workstation owned or utilized by the State or other authorized users. User access to the Services shall be routinely provided by the Vendor. All Services and information designated by Vendor as "confidential" or "proprietary" shall be kept in confidence except as may be required by the North Carolina Public Records Act: N.C.G.S. § 132-1, *et. seq.*
- b) The State's access license for the Services and its associated services neither transfers, vests, nor infers any title or other ownership right in any intellectual property rights of the Vendor or any third party, nor does this license transfer, vest, or infer any title or other ownership right in any Vendor source code associated with the Services unless otherwise agreed to by the parties. The provisions of this paragraph will not be construed as a sale of any ownership rights in the Services. Any Services or technical and business information owned by Vendor or its suppliers or licensors made accessible or furnished to the State shall be and remain the property of the Vendor or such other party, respectively. Vendor has a limited, non-exclusive license to access and use the State Data as provided to Vendor, but solely for performing its obligations under this Agreement and in confidence as provided herein.
- c) The Vendor or its suppliers shall at minimum, and except as otherwise agreed, provide telephone assistance to the State for all Services procured hereunder during the State's normal business hours (unless different hours are specified herein). The Vendor warrants that its Support and customer service and assistance will be performed in accordance with generally accepted industry standards. The State has the right to receive the benefit of upgrades, updates, maintenance releases or other enhancements or modifications made generally available to the Vendor's tenants for similar Services.
- d) The Vendor will provide to the State Services for updating, maintaining and continuing optimal performance for the Services. Unless otherwise agreed in writing, Support will also be provided for any other (e.g., third party) software provided by the Vendor in connection with the Vendor's solution herein. The technical and professional activities required for establishing, managing, and maintaining the Services environment are the responsibilities of the Vendor. Any training specified herein will be provided by the Vendor to certain State users for the fees or costs as set forth herein or in an SLA.
- e) Services provided pursuant to this Solicitation may, in some circumstances, be accompanied by a user clickwrap agreement. The term clickwrap agreement refers to an agreement that requires the end user to manifest his or her assent to terms and conditions by clicking an "ok" or "agree" button on a dialog box or pop-up window as part of the process of access to the Services. All terms and conditions of any clickwrap agreement provided with any Services solicited herein shall have no force and effect and shall be non-binding on the State, its employees, agents, and other authorized users of the Services.
- f) The Vendor may utilize partners and/or subcontractors to assist in the provision of the Services, so long as the State Data is not removed from the United States unless the terms of storage of the State Data are clearly disclosed, the security provisions referenced herein can still be complied with, and such removal is done with the prior express written permission of the State. The Vendor shall identify all of its strategic business partners related to Services provided under this contract including, but not limited to, all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Vendor, who will be involved in any application development and/or operations.
- g) The Vendor warrants that all Services will be performed with professional care and skill, in a workmanlike manner and in accordance with the Services documentation and this Agreement.

- h) Reserved..
 - i) Professional services provided by the Vendor at the request by the State in writing in addition to agreed Services shall be at the then-existing Vendor hourly rates when provided, unless otherwise agreed in writing by the parties.
- 3) **WARRANTY OF NON-INFRINGEMENT:**
- a) The Vendor warrants to the best of its knowledge that:
 - i) The Services do not infringe any intellectual property rights of any third party; and
 - ii) There are no actual or threatened actions arising from, or alleged under, any intellectual property rights of any third party.
- 4) **ACCESS AVAILABILITY; REMEDIES:**
- a) The Vendor warrants that the Services will be in good working order, and operating in conformance with Vendor's standard specifications and functions as well as any other specifications agreed to by the parties in writing, and shall remain accessible 24/7, with the exception of scheduled outages for maintenance and of other service level provisions agreed in writing, e.g., in an SLA..
 - b) The State shall notify the Vendor if the Services are not in good working order or inaccessible during the term of the Agreement. The Vendor shall, at its option, either repair, replace or reperform any Services reported or discovered as not being in good working order and accessible during the applicable contract term without cost to the State.
 - c) Support Services. Reserved..
- 5) **EXCLUSIONS:**
- a) Except as stated above in Paragraphs 3 and 4, Vendor and its parent, subsidiaries and affiliates, subcontractors and suppliers make no warranties, express or implied, as to the Services.
 - b) The warranties provided in Paragraphs 3 and 4 above do not cover repair for damages, malfunctions or service failures substantially caused by:
 - i) Actions of non-Vendor personnel;
 - ii) Failure to follow Vendor's written instructions relating to the Services provided to the State; or
 - iii) Force Majeure conditions set forth hereinbelow.
 - iv) The State's sole misuse of, or its own inability to use, the Services.
- 6) **PERFORMANCE REVIEW AND ACCOUNTABILITY:** N.C.G.S. § 143B-1340(f) and 09 NCAC 06B.1207 require provisions for performance review and accountability in State IT contracts. For this procurement, these shall include the holding a retainage of ten percent (10%) of each applicable monthly Maintenance and Enhancement value in Attachment D, plus 10% of each applicable monthly Hosting value in Attachment D, and withholding the final payment contingent on final acceptance by the State as provided in 09 NCAC 06B.1207(3) and (4), unless waived or otherwise agreed, in writing. The Services herein will be provided consistent with and under these Services performance review and accountability guarantees.
- 7) **LIMITATION OF LIABILITY: Limitation of Vendor's Contract Damages Liability:** Reserved.
- 8) **VENDOR'S LIABILITY FOR INJURY TO PERSONS OR DAMAGE TO PROPERTY:** Reserved.
- 9) **MODIFICATION OF SERVICES:** Reserved..
- 10) **TRANSITION PERIOD:**
- a) For up to six (6) months, either prior to the expiration date of this Agreement, or upon notice of termination of this Agreement, the Vendor shall assist the State, upon written request, in extracting and/or transitioning all Data, source code, and all other work products in the format determined by the State ("Transition Period").
 - b) The Transition Period may be modified in an SLA or as agreed upon in writing by the parties in a contract amendment.
 - c) During the Transition Period, Services access shall continue to be made available to the State without alteration.
 - d) The Vendor agrees to compensate the State for damages or losses the State incurs as a result of Vendor's failure to comply with this Transition Period section in accordance with the Limitation of Liability provisions above.
 - e) Upon termination, and unless otherwise stated in an SLA, and after providing the State Data to the State as indicated above in this section with acknowledged receipt by the State in writing, the Vendor shall

permanently destroy or render inaccessible any portion of the State Data in the Vendor's and/or subcontractor's possession or control following the completion and expiration of all obligations in this section. Within thirty (30) days, the Vendor shall issue a written statement to the State confirming the destruction or inaccessibility of the State's Data.

- f) The State at its option, may purchase additional Transition Services as may be agreed upon in a supplemental agreement.

11) **TRANSPORTATION:** Transportation charges for any Deliverable sent to the State other than electronically or by download shall be FOB Destination unless delivered by internet or file-transfer as agreed by the State, or otherwise specified in the solicitation document or purchase order.

12) **PAYMENT TERMS (Applicable to SaaS): Reserved.**

13) **SECURITY OF STATE DATA**

- a) All Data provided by the State to the Vendor (State Data) during the performance or provision of Services hereunder are the property of the State of North Carolina and must be kept secure and returned to the State. The Vendor will protect State Data in its hands from unauthorized disclosure, loss, damage, destruction by natural event, or other eventuality. Proprietary Vendor materials shall be identified to the State by the Vendor prior to use or provision of Services hereunder and shall remain the property of the Vendor. Derivative works of any Vendor proprietary materials prepared or created during the performance of provision of Services hereunder shall be provided to the State as part of the Services. The Vendor shall not access State User accounts, or State Data, except (i) during data center operations; (ii) in response to service or technical issues; (iii) as required by the express terms of this contract; or (iv) at the State's written request. The Vendor shall protect the confidentiality of all information, Data, instruments, studies, reports, records and other materials provided to it by the State or maintained or created in accordance with this Agreement. No such information, Data, instruments, studies, reports, records and other materials in the possession of Vendor shall be disclosed in any form without the prior written agreement with the State. The Vendor will have written policies governing access to and duplication and dissemination of all such information, Data, instruments, studies, reports, records and other materials.
- b) The Vendor shall not store or transfer non-public State data outside of the United States. This includes backup data and Disaster Recovery locations. The Service Provider will permit its personnel and contractors to access State of North Carolina data remotely only as required to provide technical support.
- c) Protection of personal privacy and sensitive data. The Vendor acknowledges its responsibility for securing any restricted or highly restricted data, as defined by the Statewide Data Classification and Handling Policy (<https://it.nc.gov/document/statewide-data-classification-and-handling-policy>) that is collected by the State and stored in any Vendor site or other Vendor housing systems including, but not limited to, computer systems, networks, servers, or databases, maintained by Vendor or its agents or subcontractors in connection with the provision of the Services. The Vendor warrants, at its sole cost and expense, that it shall implement processes and maintain the security of data classified as restricted or highly restricted; provide reasonable care and efforts to detect fraudulent activity involving the data; and promptly notify the State of any breaches of security within twenty-four (24) hours of confirmation as required by N.C.G.S. § 143B-1379.
- d) The Vendor will provide and maintain secure backup of the State Data. The Vendor shall implement and maintain secure passwords for its online system providing the Services, as well as all appropriate administrative, physical, technical and procedural safeguards at all times during the term of this Agreement to secure such Data from Data Breach, protect the Data and the Services from loss, corruption, unauthorized disclosure, and the introduction of viruses, disabling devices, malware and other forms of malicious or inadvertent acts that can disrupt the State's access to its Data and the Services. The Vendor will allow periodic back-up of State Data by the State to the State's infrastructure as the State requires or as may be provided by law.
- e) The Vendor shall certify to the State:
 - i) The sufficiency of its security standards, tools, technologies and procedures in providing Services under this Agreement;

- ii) That the system used to provide the Subscription Services under this Contract has and will maintain a valid third party security certification not to exceed one (1) year and is consistent with the data classification level and a security controls appropriate for low or moderate information system(s) per the National Institute of Standards and Technology NIST 800-53 revision 4. The State reserves the right to independently evaluate, audit, and verify such requirements.
- iii) That the Services will comply with the following:
 - (1) Any DIT security policy regarding Cloud Computing, and the DIT Statewide Information Security Policy Manual; to include encryption requirements as defined below:
 - (a) The Vendor shall encrypt all non-public data in transit regardless of the transit mechanism.
 - (b) For engagements where the Vendor stores sensitive personally identifiable or otherwise confidential information, this data shall be encrypted at rest. Examples are social security number, date of birth, driver's license number, financial data, federal/state tax information, and hashed passwords. The Vendor's encryption shall be consistent with validated cryptography standards as specified in National Institute of Standards and Technology FIPS140-2, Security Requirements. The key location and other key management details will be discussed and negotiated by both parties. When the Service Provider cannot offer encryption at rest, it must maintain, for the duration of the contract, cyber security liability insurance coverage for any loss resulting from a data breach. Additionally, where encryption of data at rest is not possible, the Vendor must describe existing security measures that provide a similar level of protection;
 - (2) Privacy provisions of the Federal Privacy Act of 1974;
 - (3) The North Carolina Identity Theft Protection Act, N.C.G.S. Chapter 75, Article 2A (e.g., N.C.G.S. § 75-65 and -66);
 - (4) The North Carolina Public Records Act, N.C.G.S. Chapter 132;
 - (5) Applicable Federal, State and industry standards and guidelines including, but not limited to, relevant security provisions of the Payment Card Industry (PCI) Data Security Standard (PCIDSS) including the PCIDSS Cloud Computing Guidelines, Criminal Justice Information, The Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA); and
 - (6) Any requirements implemented by the State under N.C.G.S. §§ 143B-1376 and -1377.
 - (7) Any requirements implemented by the State under N.C.G.S. §§ 20-309.2(d).
- f) Security Breach. "Security Breach" under the NC Identity Theft Protection Act (N.C.G.S. § 75-60 *et seq.*) means (1) any circumstance pursuant to which applicable Law requires notification of such breach to be given to affected parties or other activity in response to such circumstance (e.g., N.C.G.S. § 75-65); or (2) any actual, attempted, suspected, threatened, or reasonably foreseeable circumstance that compromises, or could reasonably be expected to compromise, either Physical Security or Systems Security (as such terms are defined below) in a fashion that either does or could reasonably be expected to permit unauthorized Processing (as defined below), use, disclosure or acquisition of or access to any the State Data or state confidential information. "Physical Security" means physical security at any site or other location housing systems maintained by Vendor or its agents or subcontractors in connection with the Services. "Systems Security" means security of computer, electronic or telecommunications systems of any variety (including data bases, hardware, software, storage, switching and interconnection devices and mechanisms), and networks of which such systems are a part or communicate with, used directly or indirectly by Vendor or its agents or subcontractors in connection with the Services. "Processing" means any operation or set of operations performed upon the State Data or State confidential information, whether by automatic means, such as creating, collecting, procuring, obtaining, accessing, recording, organizing, storing, adapting, altering, retrieving, consulting, using, disclosing or destroying.
- g) Breach Notification. In the event the Vendor becomes aware of any Security Breach due to Vendor acts or omissions other than in accordance with the terms of the Agreement, the Vendor shall, at its own expense, (1) immediately notify the State's Agreement Administrator of such Security Breach and perform a root cause analysis thereon; (2) investigate such Security Breach; (3) provide a remediation plan,

acceptable to the State, to address the Security Breach and prevent any further incidents; (4) conduct a forensic investigation to determine what systems, data and information have been affected by such event; and (5) cooperate with the State, and any law enforcement or regulatory officials, credit reporting companies, and credit card associations investigating such Security Breach. The State shall make the final decision on notifying the State's persons, entities, employees, service providers and/or the public of such Security Breach, and the implementation of the remediation plan. If a notification to a customer is required under any Law or pursuant to any of the State's privacy or security policies, then notifications to all persons and entities who are affected by the same event (as reasonably determined by the State) shall be considered legally required.

- h) Notification Related Costs. The Vendor shall issue notifications and shall pay all Notification Related Costs arising out of or in connection with any such Security Breach due to Vendor acts or omissions other than in accordance with the terms of the Agreement resulting in a requirement for legally required notifications. "Notification Related Costs" shall include costs associated with addressing and responding to the Security Breach including, but not limited to, (1) preparation and mailing or other transmission of legally required notifications; (2) preparation and mailing or other transmission of such other communications to customers, agents or others as the State deems reasonably appropriate; (3) establishment of a call center or other communications procedures in response to such Security Breach (e.g., customer service FAQs, talking points and training); (4) public relations and other similar crisis management services; (5) legal and accounting fees and expenses associated with the State's investigation of and response to such event; and (6) costs for credit reporting services that are associated with legally required notifications or are advisable, in the State's opinion, under the circumstances. If the Vendor becomes aware of any Security Breach which is not due to Vendor acts or omissions other than in accordance with the terms of the Agreement, the Vendor shall immediately notify the State of such Security Breach, and the parties shall reasonably cooperate regarding which of the foregoing or other activities may be appropriate under the circumstances, including any applicable Charges for the same.
- i) The Vendor shall allow the State reasonable access to Services security logs, latency statistics, and other related Services security data that affect this Agreement and the State's Data, at no cost to the State.
- j) In the course of normal operations, it may become necessary for the Vendor to copy or move Data to another storage destination on its online system, and delete the Data found in the original location. In any such event, the Vendor shall preserve and maintain the content and integrity of the Data, except by prior written notice to, and prior written approval by, the State.
- k) Remote access to Data from outside the continental United States including, without limitation, remote access to Data by authorized Services support staff in identified support centers, is prohibited unless approved in advance by the State Chief Information Officer or the Using Agency.
- l) In the event of temporary loss of access to Services, the Vendor shall promptly restore continuity of Services, restore Data in accordance with this Agreement and as may be set forth in an SLA, restore accessibility of Data and the Services to meet the performance requirements stated herein or in an SLA. As a result, Service Level remedies will become available to the State as provided herein, in the SLA or other agreed and relevant documents. Failure to promptly remedy any such temporary loss of access may result in the State exercising its options for assessing damages under this Agreement.
- m) In the event of disaster or catastrophic failure that results in significant State Data loss or extended loss of access to Data or Services, the Vendor shall notify the State by the fastest means available and in writing, with additional notification provided to the State Chief Information Officer or designee of the contracting agency. Vendor shall provide such notification within twenty-four (24) hours after Vendor reasonably believes there has been such a disaster or catastrophic failure. In the notification, Vendor shall inform the State of:
 - (1) The scale and quantity of the State Data loss;
 - (2) What Vendor has done or will do to recover the State Data from backups and mitigate any deleterious effect of the State Data and Services loss; and
 - (3) What corrective action Vendor has taken or will take to prevent future State Data and Services loss.
 - (4) If Vendor fails to respond immediately and remedy the failure, the State may exercise its options for assessing damages or other remedies under this Agreement.

The Vendor shall investigate the disaster or catastrophic failure and shall share the report of the investigation with the State. The State and/or its authorized agents shall have the right to lead (if required by law) or participate in the investigation. The Vendor shall cooperate fully with the State, its agents and law enforcement.

- n) In the event of termination of this contract, cessation of business by the Vendor or other event preventing the Vendor from continuing to provide the Services, the Vendor shall not withhold the State Data or any other State confidential information or refuse, for any reason, to promptly return to the State the State Data and any other State confidential information (including copies thereof) if requested to do so on such media as reasonably requested by the State, even if the State is then or is alleged to be in breach of the Agreement. As a part of the Vendor's obligation to provide the State Data pursuant to this Paragraph 18) n), the Vendor will also provide the State any data maps, documentation, software, or other materials necessary, including, without limitation, handwritten notes, materials, working papers or documentation, for the State to use, translate, interpret, extract and convert the State Data.
- o) Secure Data Disposal. When requested by the State, the Vendor shall destroy all requested data in all of its forms (e.g., disk, CD/DVD, backup tape, and paper). Data shall be permanently deleted and shall not be recoverable, in accordance with National Institute of Standards and Technology (NIST) approved methods, and certificates of destruction shall be provided to the State.

Section 3: Terms and Conditions Applicable to Personnel and Personal Services

- 1) **VENDOR'S REPRESENTATION:** Vendor warrants that qualified personnel will provide Services in a professional manner. "Professional manner" means that the personnel performing the Services will possess the skill and competence consistent with the prevailing business standards in the information technology industry. Vendor agrees that it will not enter any agreement with a third party that might abridge any rights of the State under the Agreement. Vendor will serve as the prime Vendor under the Agreement. Should the State approve any subcontractor(s), the Vendor shall be legally responsible for the performance and payment of the subcontractor(s). Names of any third party Vendors or subcontractors of Vendor may appear for purposes of convenience in Contract documents; and shall not limit Vendor's obligations hereunder. Such third party subcontractors, if approved, may serve as subcontractors to Vendor. Vendor will retain executive representation for functional and technical expertise as needed in order to incorporate any work by third party subcontractor(s).
 - a) Intellectual Property. Vendor represents that it has the right to provide the Services and other Deliverables without violating or infringing any law, rule, regulation, copyright, patent, trade secret or other proprietary right of any third party. Vendor also represents that its Services and other Deliverables are not the subject of any actual or threatened actions arising from, or alleged under, any intellectual property rights of any third party.
 - b) Inherent Services. If any Services or other Deliverables, functions, or responsibilities not specifically described in the Agreement are required for Vendor's proper performance, provision and delivery of the Services and other Deliverables pursuant to the Agreement, or are an inherent part of or necessary sub-task included within the Services, they will be deemed to be implied by and included within the scope of the Contract to the same extent and in the same manner as if specifically described in the Contract.
 - c) Vendor warrants that it has the financial capacity to perform and to continue to perform its obligations under the Contract; that Vendor has no constructive or actual knowledge of an actual or potential legal proceeding being brought against Vendor that could materially adversely affect performance of the Agreement; and that entering into the Agreement is not prohibited by any Contract, or order by any court of competent jurisdiction.
- 2) **SERVICES PROVIDED BY VENDOR:** Vendor shall provide the State with implementation Services as specified in a Statement of Work ("SOW") executed by the parties. This Agreement in combination with each SOW individually comprises a separate and independent contractual obligation from any other SOW. A breach by Vendor under one SOW will not be considered a breach under any other SOW. The Services intended hereunder are related to the State's implementation and/or use of one or more

Software Deliverables licensed hereunder or in a separate software license agreement between the parties ("License Agreement"). (Reserve if not needed)

- 3) **PERSONNEL**: Vendor shall not substitute key personnel assigned to the performance of the Agreement without prior written approval by the Agency Contract Administrator. The individuals designated as key personnel for purposes of the Agreement are those specified in the Vendor's offer. Any desired substitution shall be noticed to the Agency's Contract Administrator in writing accompanied by the names and references of Vendor's recommended substitute personnel. The Agency will approve or disapprove the requested substitution in a timely manner. The Agency may, in its sole discretion, terminate the Services of any person providing Services under the Agreement. Upon such termination, the Agency may request acceptable substitute personnel or terminate the Contract Services provided by such personnel.
- a) Unless otherwise expressly provided in the Contract, Vendor will furnish all of its own necessary management, supervision, labor, facilities, furniture, computer and telecommunications equipment, software, supplies and materials necessary for the Vendor to provide and deliver the Services and other Deliverables.
 - b) Vendor personnel shall perform their duties on the premises of the State, during the State's regular work days and normal work hours, except as may be specifically agreed otherwise, established in the specification, or statement of work.
 - c) The Agreement shall not prevent Vendor or any of its personnel supplied under the Agreement from performing similar Services elsewhere or restrict Vendor from using the personnel provided to the State, provided that:
 - i) Such use does not conflict with the terms, specifications or any amendments to the Agreement, or
 - ii) Such use does not conflict with any procurement law, regulation or policy, or
 - iii) Such use does not conflict with any non-disclosure agreement, or term thereof, by and between the State and Vendor or Vendor's personnel.
 - d) Unless otherwise provided by the Agency, the Vendor shall furnish all necessary personnel, Services, and otherwise perform all acts, duties and responsibilities necessary or incidental to the accomplishment of the tasks specified in the Agreement. The Vendor shall be legally and financially responsible for its personnel including, but not limited to, any deductions for social security and other withholding taxes required by state or federal law. The Vendor shall be solely responsible for acquiring any equipment, furniture, and office space not furnished by the State necessary for the Vendor to comply with the Agreement. The Vendor personnel shall comply with any applicable State facilities or other security rules and regulations.
- 4) **PERSONAL SERVICES**: The State shall have and retain the right to obtain personal Services of any individuals providing Services under the Agreement. This right may be exercised at the State's discretion in the event of any transfer of the person providing personal Services, termination, default, merger, acquisition, bankruptcy or receivership of the Vendor to ensure continuity of Services provided under the Agreement. Provided, however, that the Agency shall not retain or solicit any Vendor employee for purposes other than completion of personal Services due as all or part of any performance due under the Agreement.
- a) Vendor personnel shall perform any duties on the premises of the State during the State's regular work days and normal work hours, except as may be specifically agreed otherwise, established in the specification, or statement of work.
 - b) The State has and reserves the right to disapprove the continuing assignment of Vendor personnel provided by Vendor under the Agreement. If this right is exercised and the Vendor is not able to replace the disapproved personnel as required by the State, the parties agree to employ best commercial efforts to informally resolve such failure equitably by adjustment of other duties, set-off, or modification to other terms that may be affected by Vendor's failure.
 - c) Vendor will make every reasonable effort consistent with prevailing business practices to honor the specific requests of the State regarding assignment of Vendor's employees. Vendor reserves the sole right to determine the assignment of its employees. If one of Vendor's employees is unable to

perform due to illness, resignation, or other factors beyond Vendor's control, Vendor will provide suitable personnel at no additional cost to the State.

- d) The Agreement shall not prevent Vendor or any of its personnel supplied under the Agreement from performing similar Services elsewhere or restrict Vendor from using the personnel provided to the State, provided that:
 - i) Such use does not conflict with the terms, specifications or any amendments to the Agreement, or
 - ii) Such use does not conflict with any procurement law, regulation or policy, or
 - iii) Such use does not conflict with any non-disclosure agreement, or term thereof, by and between the State and Vendor or Vendor's personnel.

Section 4: Terms and Conditions Applicable to Information Technology Goods and Services

- 1) **SOFTWARE LICENSE FOR HARDWARE, EMBEDDED SOFTWARE AND FIRMWARE:** Deliverables comprising goods, equipment or products (hardware) may contain software for internal operation, or as embedded software or firmware that is generally not sold or licensed as a severable software product. Software may be provided on separate media, such as a CD-ROM or other media, or may be included within the hardware at or prior to delivery. Such software is proprietary, copyrighted, and may also contain valuable trade secrets and may be protected by patents. Vendor grants the State a license to use the Code (or any replacement provided) on, or in conjunction with, only the Deliverables purchased, or with any system identified in the solicitation documents. The State shall have a worldwide, nonexclusive, non-sublicensable license to use such software and/or documentation for its internal use. The State may make and install copies of the software to support the authorized level of use. Provided, however that if the hardware is inoperable, the software may be copied for temporary use on other hardware. The State shall promptly affix to any such copy the same proprietary and copyright notices affixed to the original. The State may make one copy of the software for archival, back-up or disaster recovery purposes. The license set forth in this Paragraph shall terminate immediately upon the State's discontinuance of the use of all equipment on which the software is installed. The software may be transferred to another party only with the transfer of the hardware. If the hardware is transferred, the State shall i) destroy all software copies made by the State, ii) deliver the original or any replacement copies of the software to the transferee, and iii) notify the transferee that title and ownership of the software and the applicable patent, trademark, copyright, and other intellectual property rights shall remain with Vendor, or Vendor's licensors. The State shall not disassemble, decompile, reverse engineer, modify, or prepare derivative works of the embedded software, unless permitted under the solicitation documents.
- 2) **LICENSE GRANT FOR APPLICATION SOFTWARE, (COTS):** This paragraph recites the scope of license granted, if not superseded by a mutually agreed and separate licensing agreement, as follows:
 - a) Vendor grants to the State, its Agencies and lawful customers a non-exclusive, non-transferable and non-sublicensable license to use, in object code format, Vendor's software identified in the solicitation documents, Vendor's Statement of Work (SOW), or an Exhibit thereto executed by the parties ("Software"), subject to the restrictions set forth therein, such as the authorized computer system, the data source type(s), the number of target instance(s) and the installation site. Use of the Software shall be limited to the data processing and computing needs of the State, its Agencies and lawful customers. This license shall be perpetual unless terminated as provided herein. The State agrees not to distribute, sell, sublicense or otherwise transfer copies of the Software or any portion thereof. For purposes of this Agreement, a State Entity shall be defined as any department or agency of the State of North Carolina, which is controlled by or under common control of the State or who is a lawful customer of the State pursuant to Article 3D of Chapter 147 of the General Statutes.
 - b) Vendor shall provide all encryption or identification codes or authorizations that are necessary or proper for the operation of the licensed Software.

- c) The State shall have the right to copy the Software, in whole or in part, for use in conducting benchmark or acceptance tests, for business recovery and disaster recovery testing or operations, for archival or emergency purposes, for back up purposes, for use in preparing derivative works if allowed by the solicitation documents or statements of work, or to replace a worn copy.
 - d) The State may modify non-personal Software in machine-readable form for its internal use in merging the same with other software program material. Any action hereunder shall be subject to uses described in this paragraph, the restrictions imposed by Paragraph 3), and applicable terms in the solicitation documents or statements of work.
- 3) **WARRANTY TERMS:** Notwithstanding anything in the Agreement or Exhibit hereto to the contrary, Vendor shall assign warranties for any Deliverable supplied by a third party to the State.
- a) a) Vendor warrants that any Software or Deliverable will operate substantially in conformity with prevailing specifications as defined by the current standard documentation (except for minor defects or errors which are not material to the State) for a period of ninety (90) days from the date of acceptance ("Warranty Period"), unless otherwise specified in the Solicitation Documents. If the Software does not perform in accordance with such specifications during the Warranty Period, Vendor will use reasonable efforts to correct any deficiencies in the Software so that it will perform in accordance with or substantially in accordance with such specifications.
 - b) Vendor warrants to the best of its knowledge that:
 - i) The licensed Software and associated materials do not infringe any intellectual property rights of any third party;
 - ii) There are no actual or threatened actions arising from, or alleged under, any intellectual property rights of any third party;
 - iii) The licensed Software and associated materials do not contain any surreptitious programming codes, viruses, Trojan Horses, "back doors" or other means to facilitate or allow unauthorized access to the State's information systems.
 - iv) The licensed Software and associated materials do not contain any timer, counter, lock or similar device (other than security features specifically approved by Customer in the Specifications) that inhibits or in any way limits the Software's ability to operate.
 - c) UNLESS MODIFIED BY AMENDMENT OR THE SOLICITATION DOCUMENTS, THE WARRANTIES IN THIS PARAGRAPH ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, OR WHETHER ARISING BY COURSE OF DEALING OR PERFORMANCE, CUSTOM, USAGE IN THE TRADE OR PROFESSION OR OTHERWISE, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NO OTHER REPRESENTATIONS OR WARRANTIES HAVE FORMED THE BASIS OF THE BARGAIN HEREUNDER.
- 4) **RESTRICTIONS:** State's use of the Software is restricted as follows:
- a) The license granted herein is granted to the State and to any political subdivision or other entity permitted or authorized to procure Information Technology through the Department of Information Technology. If the License Grant and License Fees are based upon the number of Users, the number of Users may be increased at any time, subject to the restrictions on the maximum number of Users specified in the solicitation documents.
 - b) No right is granted hereunder to use the Software to perform Services for commercial third parties (so-called "service bureau" uses). Services provided to other State Departments, Agencies or political subdivisions of the State is permitted.
 - c) The State may not copy, distribute, reproduce, use, lease, rent or allow access to the Software except as explicitly permitted under this Agreement, and State will not modify, adapt, translate, prepare derivative works (unless allowed by the solicitation documents or statements of work,) decompile, reverse engineer, disassemble or otherwise attempt to derive source code from the Software or any internal data files generated by the Software.
 - d) State shall not remove, obscure or alter Vendor's copyright notice, trademarks, or other proprietary rights notices affixed to or contained within the Software.

- 5) **SUPPORT OR MAINTENANCE SERVICES**: This paragraph recites the scope of maintenance Services due under the license granted, if not superseded by a separate licensing and maintenance agreement or as may be stated in the solicitation documents. Subject to payment of a Support Service or Maintenance Fee stated in the solicitation documents for the first year and all subsequent years, if requested by the State, Vendor agrees to provide the following support Services ("Support Services") for the current version and one previous version of the Software commencing upon delivery of the Software:
- a) **Error Correction**: If the error conditions reported by the State pursuant to the General Terms and Conditions are not corrected in a timely manner, the State may request a replacement copy of the licensed Software from Vendor. In such event, Vendor shall then deliver a replacement copy, together with corrections and updates, of the licensed Software within 24 hours of the State's request at no added expense to the State.
 - b) **Other Agreement**: This Paragraph 5 may be superseded by written mutual agreement provided that: Support and maintenance Services shall be fully described in such a separate agreement annexed hereto and incorporated herein
 - c) **Temporary Extension of License**: If any licensed Software or CPU/computing system on which the Software is installed fails to operate or malfunctions, the term of the license granted shall be temporarily extended to another CPU selected by the State and continue until the earlier of:
 - i) Return of the inoperative CPU to full operation, or
 - ii) Termination of the license.
 - d) **Encryption Code**: Vendor shall provide any temporary encryption code or authorization necessary or proper for operation of the licensed Software under the foregoing temporary license. The State will provide notice by expedient means, whether by telephone, e-mail or facsimile of any failure under this paragraph. On receipt of such notice, Vendor shall issue any temporary encryption code or authorization to the State within twenty-four (24) hours; unless otherwise agreed.
 - e) **Updates**: Vendor shall provide to the State, at no additional charge, all new releases and bug fixes (collectively referred to as "Updates") for any Software Deliverable developed or published by Vendor and made generally available to its other customers at no additional charge. All such Updates shall be a part of the Program and Documentation and, as such, be governed by the provisions of the Agreement.
 - f) **Telephone Assistance**: Vendor shall provide the State with telephone access to technical support engineers for assistance in the proper installation and use of the Software, and to report and resolve Software problems, during normal business hours, 7:30 AM - 5:30 PM Eastern Time, Monday-Friday. Vendor shall respond to the telephone requests for Program maintenance service, within four (4) business hours

Attachment C – Description of Offeror

Attachment C – Description of Offeror is provided on the following pages.

ATTACHMENT C: DESCRIPTION OF OFFEROR

Provide the information about the offeror.

Offeror's full name	Voyatek
Offeror's address	9175 Guilford Rd, Suite 218, Columbia, MD 21046 (Howard county)
Offeror's telephone number	443-276-4788
Ownership	☐ Public ☐ Partnership ☐ Subsidiary ☒ Other (specify) - LLC
Date established	2005
If incorporated, State of incorporation.	N/A
North Carolina Secretary of State Registration Number, if currently registered	Customer Number 44183
Number of full-time employees on January 1 st for the last three years or for the duration that the Vendor has been in business, whichever is less.	797
Offeror's Contact for Clarification of offer: Contact's name Title Email address and Telephone Number	Jay Saunders Vice President Jay.Saunders@Voyatek.com 913-707-0389
Offeror's Contact for Negotiation of offer: Contact's name Title Email address and Telephone Number	Jay Saunders Vice President Jay.Saunders@Voyatek.com 913-707-0389
If Contract is Awarded, Offeror's Contact for Contractual Issues: Contact's name Title Email address and Telephone Number	Kevin Rodkey Dep. General Counsel & VP Contract Management Kevin.Rodkey@voyatek.com 443-812-2152
If Contract is Awarded, Offeror's Contact for Technical Issues: Contact's name Title Email address and Telephone Number	Krushanu Majmundar Vice President Krushanu.Majmundar@voyatek.com 410-258-1144

Attachment D – Cost Form

Attachment D – Cost Form is provided on the following pages.

ATTACHMENT D: COST FORM

Vendors will submit all Crossroads pricing with the technical response, but in a separate area that allows cost and pricing information to be partitioned separately from other documents. All electronic submission forms will also separate the cost and pricing from the technical proposals.

Total Cost Summary: Vendors will include a Total Cost Summary Table in addition to the costs provided in each of the detailed cost tables. The Total Cost Summary Table will include total cost including all deliverables, with the exception of optional services. The evaluation of cost proposal responses will be based on the Table 1 summary table. Vendors are responsible for ensuring that the Total Cost Summary Table accurately reflects the cost in each of the individual pricing tables

Cost Table 1 - Total Cost of Contract

Description	Total Cost
Transition-In Phase Cost (from Cost Table 2)	\$ 142,500.00
Total Annual M&E Phase Cost – Contract Years 1-10 (from Cost Table 3)	\$ 11,111,908.00
Total Annual Hosting Costs – Contract Years 1-10 (from Cost Table 4)	\$ 4,627,244.00
Transition-Out Period Cost (from Cost Table 5)	\$ 0.00
Total Document Deliverable Cost (from Cost Table 6)	\$ 0.00
Supplemental Services Hours Contract Years 1-10 (from Cost Table 7)	\$ 753,500.00
Total Ten-Year Cost	\$ 16,635,152.00

Cost Table 1a. Total Cost by Contract Term

Contract Term	Total Cost
Initial seven (7) year Contract Term	\$10,339,488.00
Optional Renewal Term 1 (Contract year 8)	\$ 1,793,052.00
Optional Renewal Term 2 (Contract year 9)	\$ 1,846,848.00
Optional Renewal Term 3 (Contract year 10)	\$ 1,902,264.00
Total Contract Cost including Optional Renewal Terms	\$15,881,652.00

1.1. Price for Crossroads Transition-In, Annual Maintenance, and Transition-Out

Provide the Vendor's proposed maintenance pricing for each year of the Contract, not including the Supplemental Service Hours.

Cost Table 2 - Pricing for Transition-In Phase (Deliverables 1.x)

Transition-In Month	Monthly Transition-In Cost
Month 1	\$ 10,000.00
Month 2	\$ 10,000.00
Month 3	\$ 20,000.00
Month 4	\$ 20,500.00
Month 5	\$ 20,500.00
Month 6	\$ 20,500.00
Month 7	\$ 20,500.00
Month 8	\$ 20,500.00
Total Transition-In Phase Cost	\$142,500.00

Cost Table 3 - Pricing for Crossroads Annual Maintenance and Enhancement Phase (Deliverables 6.x)

Description	Monthly M&E Cost	Multiplier	Total Fixed Annual M&E Cost
Contract Year 1	\$85,240.00	4	\$ 340,960.00
Contract Year 2	\$88,352.00	12	\$ 1,060,224.00
Contract Year 3	\$91,003.00	12	\$ 1,092,036.00
Contract Year 4	\$93,733.00	12	\$ 1,124,796.00
Contract Year 5	\$96,545.00	12	\$ 1,158,540.00
Contract Year 6	\$99,441.00	12	\$ 1,193,292.00
Contract Year 7	\$102,424.00	12	\$ 1,229,088.00
Optional Contract Year 8	\$105,497.00	12	\$ 1,265,964.00
Optional Contract Year 9	\$108,662.00	12	\$ 1,303,944.00
Optional Contract Year 10	\$111,922.00	12	\$ 1,343,064.00
Total Ten Year M&E Phase			\$ 11,111,908.00

Cost Table 4 - Pricing for Crossroads Annual Hosting (Deliverables 21.x)

Description	Monthly or Annual Hosting Cost	Multiplier	Total Fixed Annual Hosting Cost
Contract Year 1	\$ 35,690.00	4 mo	\$ 142,760.00
Contract Year 2	\$ 36,785.00	12 mo or 1 yr	\$ 441,420.00
Contract Year 3	\$ 37,889.00	12 mo or 1 yr	\$ 454,668.00
Contract Year 4	\$ 39,025.00	12 mo or 1 yr	\$ 468,300.00
Contract Year 5	\$ 40,196.00	12 mo or 1 yr	\$ 482,352.00
Contract Year 6	\$ 41,402.00	12 mo or 1 yr	\$ 496,824.00
Contract Year 7	\$ 42,644.00	12 mo or 1 yr	\$ 511,728.00
Optional Contract Year 8	\$ 43,924.00	12 mo or 1 yr	\$ 527,088.00
Optional Contract Year 9	\$ 45,242.00	12 mo or 1 yr	\$ 542,904.00
Optional Contract Year 10	\$ 46,600.00	12 mo or 1 yr	\$ 559,200.00
Total Ten Year Hosting Cost			\$ 4,627,244.00

Cost Table 5 - Pricing for Transition-Out Period – Fixed Amount (Deliverable 16)

Transition-Out Period (inclusive of completion of all Transition-Out Period tasks and submission of the Transition-Out Completion Report)	\$0

1.2. Price for Crossroads Deliverables

There are deliverables that are needed to ensure a successful release deployments and operations of the NC WIC Crossroads System. Payment will only be made for the deliverables listed below after unconditional acceptance by the State. Acceptance by the State will be in the form of a written acknowledgement that the Deliverable meets the requirements. Provide the Vendor's proposed pricing for each of the deliverables listed in Price Table 6 below.

Cost Table 6 - Pricing for Product Deliverables

Deliverable ID	Deliverable Name	Price
3B	Work Plan and Schedule FINAL	\$ 0
9	Production Deployment Plan	\$ 0
Total Deliverable Cost		\$ 0

1.3. Supplemental Services

The State will require the Vendor to provide Supplemental Services, for completion and deployment of Changes Requests. Vendors will provide Change Request cost estimates using the blended hourly resource pricing for each of the Contract Years one (1) through seven (7) and optional years one (1) through three (3) in Price Table 7 below. Hours are invoiced as utilized in accordance with the Change Request process.

Cost Table 7 - Pricing of Supplemental Services

Description	# Change Request Hours	Blended Hourly Rate	Total Cost
Contract Years 1-7	3500	\$ 148	\$ 518,000
Optional Contract Year 8	500	\$ 152	\$ 76,000
Optional Contract Year 9	500	\$ 157	\$ 78,500
Optional Contract Year 10	500	\$ 162	\$ 81,000
Total Ten Year Supplemental Services Cost			\$ 753,500

1.4. Other Optional Services

Vendors are encouraged to propose other optional technical services that may improve efficiency and/or effectiveness to the Crossroads system, its interfaces to 3rd party solutions, or NC WIC Program as a whole. For example, vendors may propose an optional service for a mobile phone application, to be used by participants to access benefit and other WIC information, and/or other optional services that may be beneficial to the program and stakeholders.

Optional services may be bid to be implemented upon contract award or may be initiated in any of the contract years. The Other Optional Services must be compliant with all security and enterprise specifications under Section 3.0, described in enough detail for North Carolina to evaluate the services, and any associated pricing will be separate from the pricing for the Crossroads Scope of Work sections. A narrative description will be provided for each optional service, including a description, information on

other states' programs that have implemented the service, why it would be advantageous for NC, and the cost broken out by industry standards and/or monthly/annually, as applicable. Each optional service must be included separately in the narrative and cost proposal.

Vendors may add as many rows as needed to Cost Table 8 for optional services proposed, and may include annual pricing. The State must not be charged for any optional services unless such optional services are specifically requested by the State in writing.

Cost Table 8 - Proposed Optional Services Pricing

Optional Service Proposed	Pricing
Supplemental Perfective Developer	\$ 267,033 Per Year
Data and Reporting Analyst	\$ 240,326 Per Year
Mobile Application - Standard	\$ 130,000
Mobile Application – Upload Documents	\$ 42,000
Mobile Application – Appointment Method	\$ 30,000
Mobile Application – UPC Submit	\$ 42,000
Mobile Application – Manage Multiple Cards	\$ 17,500
Mobile Application – Capture Signatures	\$ 60,000
Mobile Application – Redemption Dashboard	\$ 36,000
Mobile Application –OPT for Passwords (requires SMS subscription)	\$ 22,000
Mobile Application –Custom Nutrition Education	\$ 75,000
Farmers Market	\$ 270,000 (state retains rights)
Penetration Testing	\$ 35,000 per test
TeleHealth Services – Setup and Integration	\$ 150,000 Setup and Integration, \$ 12,000 per month for 8,000 hours of video conferencing.
TeleHealth Services – Per 10,000 hours of meetings or 100,000 SMS messages. Additional volume pricing can be calculated as needed.	\$ 12,000 per month for 10,000 hours of video conferencing. \$ 3,500 per month for 100,000 SMS messages

Attachment E – Vendor Certification Form

Attachment E – Vendor Certification Form is provided on the following pages.

ATTACHMENT E: VENDOR CERTIFICATION FORM

1) ELIGIBLE VENDOR

The Vendor certifies that in accordance with N.C.G.S. §143-59.1(b), Vendor is not an ineligible vendor as set forth in N.C.G.S. §143-59.1 (a).

The Vendor acknowledges that, to the extent the awarded contract involves the creation, research, investigation or generation of a future RFP or other solicitation; the Vendor will be precluded from bidding on the subsequent RFP or other solicitation and from serving as a subcontractor to an awarded vendor.

The State reserves the right to disqualify any bidder if the State determines that the bidder has used its position (whether as an incumbent Vendor, or as a subcontractor hired to assist with the RFP development, or as a Vendor offering free assistance) to gain a competitive advantage on the RFP or other solicitation.

2) CONFLICT OF INTEREST

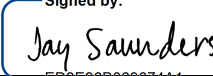
Applicable standards may include: N.C.G.S. §§143B-1352 and 143B-1353, 14-234, and 133-32. The Vendor shall not knowingly employ, during the period of the Agreement, nor in the preparation of any response to this solicitation, any personnel who are, or have been, employed by a Vendor also in the employ of the State and who are providing Services involving, or similar to, the scope and nature of this solicitation or the resulting contract.

3) E-VERIFY

Pursuant to N.C.G.S. § 143B-1350(k), the State shall not enter into a contract unless the awarded Vendor and each of its subcontractors comply with the E-Verify requirements of N.C.G.S. Chapter 64, Article 2. Vendors are directed to review the foregoing laws. Vendors claiming exceptions or exclusions under Chapter 64 must identify the legal basis for such claims and certify compliance with federal law regarding registration of aliens including 8 USC 1373 and 8 USC 1324a. Any awarded Vendor must submit a certification of compliance with E-Verify to the awarding agency, and on a periodic basis thereafter as may be required by the State.

4) CERTIFICATE TO TRANSACT BUSINESS IN NORTH CAROLINA

As a condition of contract award, awarded Vendor shall have registered its business with the North Carolina Secretary of State and shall maintain such registration throughout the term of the Contract.

Signed by: 
Signature: _____ Date: 1/17/2025

Printed Name: Jay Saunders Title: Vice President

Attachment F – Location of Workers Utilized

Attachment F – Location of Workers Utilized is provided on the following pages.

ATTACHMENT F: LOCATION OF WORKERS UTILIZED BY VENDOR

In accordance with N.C.G.S. §143B-1361(b), Vendor must identify how it intends to utilize resources or workers located outside the U.S., and the countries or cities where such are located. The State will evaluate additional risks, costs, and other factors associated with the Vendor's utilization of resources or workers prior to making an award for any such Vendor's offer. The Vendor shall provide the following:

- a) The location of work to be performed by the Vendor's employees, subcontractors, or other persons, and whether any work will be performed outside the lower 48 contiguous United States. The Vendor shall provide notice of any changes in such work locations if the changes result in performing work outside of the contiguous United States.
- b) Any Vendor or subcontractor providing support or maintenance Services for software, call or contact center Services shall disclose the location from which the call or contact center Services are being provided upon request.

Will Vendor perform any work outside of the contiguous United States?

☐ YES ☒ NO

If yes, Vendor MUST list what countries the employees are working and in what capacity are they accessing State Data. Specifically, the State must know if the employees are Help Desk support, Technical Support and/or Coder, etc.

Attachment G – References

In response to the requirement for customer references, please find Attachment G in the following pages, which includes three (3) references of customers who have fully implemented the proposed solution within the last three (3) years. These references are from communities and industries similar to those in North Carolina, specifically Rhode Island, South Carolina, and Maryland. Each reference includes the customer's contact information, implementation details, and support metrics.

ATTACHMENT G: REFERENCES

The Vendor shall provide three (3) references of customers utilizing the proposed solution fully implemented in a setting similar to this solicitation's scope of work. References within like North Carolina communities / industries are encouraged.

The Vendor should have implemented the respective proposed service within the last three (3) years. Customer references whose business processes and data needs are similar to those performed by the Agency needing this solution in terms of functionality, complexity, and transaction volume are encouraged.

For each reference, the Vendor shall provide the following information:

- a. Customer name.
- b. Customer address.
- c. Current telephone number of a customer employee most familiar with the offered solution implementation.
- d. Customer email address
- e. Time period over which each offered solution implementation was completed.
- f. Brief summary of the offered solution implementation.
- g. List of offered solution products installed and operational.
- h. Number of vendor or technical staff supporting, maintaining and managing the offered solution
- i. Number of end users supported by the offered solution.
- j. Number of sites supported by the offered solution.

Voyatek's three references are below for North Carolina's consideration:



Maryland WIC MIS Maintenance & Operation

Voyatek has been providing WIC operational maintenance services and enhancements for the State of Maryland since 2005. As our first WIC customer, Maryland holds a special place in the history of Voyatek. It was on this contract that our staff learned about the benefits of WIC to the participants and the dedication of the state, local agency, and clinic staff to the mission of WIC. We have included Maryland as a reference because it demonstrates our long-term commitment to the WIC Program. **Table 1** below contains the requested prior experience details.

Table 1: Prior Experience with Maryland WIC

Customer	Maryland WIC
Customer Address	201 West Preston Street, Baltimore, MD 21201
Contact Person Name & Title	Jennifer Wilson, WIC Director
Contact Person Phone Number	301-957-1148
Contact Person E-mail Address	jennifer.wilson@maryland.gov
Time Period and Services Provided	Operational support, maintenance services and enhancements for the State of Maryland's WIC MIS since 2005 (several contracts) including mobile app and participant portal.
Number of Technical Staff	10
Number of End Users Supported	300
Number of Sites Supported	85 clinics plus the state office



Rhode Island WIC MIS Maintenance & Operation

Voyatek has been providing WIC operational maintenance services and enhancements including cloud hosting in the Microsoft Azure cloud for the State of Rhode Island's Crossroads WIC MIS since 2024 for the Virginia-led Crossroads User Group (VA, AL, RI, & WV). We have included Rhode Island as a reference because, like North Carolina, they wanted their instance of Crossroads to be hosted in the cloud. Voyatek will be following a similar process for North Carolina as we did for Rhode Island in migrating and transitioning the Crossroads environments and systems to the Azure cloud. **Table 2** below contains the requested prior experience details.

Table 2: Prior Experience with Rhode Island WIC

Customer	Rhode Island WIC
Customer Address	3 Capitol Hill, Room 302, Providence, RI 02908
Contact Person Name & Title	Ann Barone, WIC Director
Contact Person Phone Number	401-222-4642
Contact Person E-mail Address	Ann.Barone@health.ri.gov
Time Period and Services Provided	Operational support, maintenance services and enhancements, and cloud hosting for the State of Rhode Island's WIC MIS since 2024.
Number of Technical Staff	3 (portion of the Crossroads User Group support team)
Number of End Users Supported	Approximately 125
Number of Sites Supported	25 clinics plus the State Office



South Carolina WIC MIS Maintenance & Operation

Voyatek has been providing WIC operational maintenance services and enhancements for the State of South Carolina since 2018. We have included South Carolina as a reference because we provide system hosting for South Carolina also, but for a different system and in an on-premises data center. **Table 3** below contains the requested prior experience details.

Table 3: Prior Experience with South Carolina WIC

Customer	South Carolina WIC
Customer Address	2100 Bull Street, Columbia, SC 29201
Contact Person Name & Title	Berry Kelly, WIC Director
Contact Person Phone Number	803-893-0743
Contact Person E-mail Address	kellybb@dph.sc.gov
Time Period and Services Provided	Operational support, maintenance services and enhancements, and hosting for the State of South Carolina's WIC MIS since 2018 including mobile app and TeleWIC telehealth system.
Number of Technical Staff	5
Number of End Users Supported	Approximately 1000
Number of Sites Supported	70 clinics and 5 primary care centers plus the State Office

Attachment H – Financial Review Form

Attachment H – Financial Review Form is provided on the following pages.

ATTACHMENT H: FINANCIAL REVIEW FORM

Vendor shall review the Financial Review Form, provide responses in the gray-shaded boxes, and submit the completed Form as an Excel file with its offer. Vendor shall not add or delete rows or columns in the Form, or change the order of the rows or column in the file.

1. Vendor Name: **GCOM Software LLC d/b/a Voyatek**

2. Company structure for tax purposes (C Corp, S Corp, LLC, LLP, etc.): **LLC**

3. Have you been in business for more than three years? ☒ **Yes** ☐ **No**

4. Have you filed for bankruptcy in the past three years? ☐ **Yes** ☒ **No**

5. In the past three years, has your auditor issued any notification letters addressing significant issues? If yes, please explain and provide a copy of the notification letters. ☐ **Yes** ☒ **No**

6. Are the financial figures below based on audited financial statements? ☒ **Yes** ☒ **No**

Yes 2022 & 2023 | No 2024

7. Start Date of financial statements: **01/01/2022**

End Date of financial statements: **12/31/2024**

8. Provide a link to annual reports with financial statements and management discussion for the past three complete fiscal years: **Not applicable for Voyatek, a private company**

9. Provide the following information for the past three complete fiscal years:

	Latest complete fiscal year minus two years	Latest complete fiscal year minus one year	Latest complete fiscal year
BALANCE SHEET DATA			
a. Cash and Temporary Investments	\$1,278	\$14,522	\$7,004
b. Accounts Receivable (beginning of year)	\$52,472	\$42,336	\$84,862
c. Accounts Receivable (end of year)	\$42,336	\$84,862	\$95,167
d. Average Account Receivable for the Year (calculated)	\$47,404	\$63,599	\$90,014
e. Inventory (beginning of year)	\$	\$	\$
f. Inventory (end of year)	\$	\$	\$
g. Average Inventory for the Year (calculated)	\$	\$	\$
h. Current Assets	\$45,578	\$101,222	\$104,280
i. Current Liabilities	\$61,495	\$92,642	\$95,501
j. Total Liabilities	\$256,921	\$597,114	\$647,581
k. Total Stockholders' Equity (beginning of year)	\$3,239	-\$41,531	\$23,951
l. Total Stockholders' Equity (end of year)	-\$41,531	\$23,951	-\$74,196
m. Average Stockholders' Equity during the year (calculated)	-\$19,146	-\$8,790	-\$25,122
INCOME STATEMENT DATA			
a. Net Sales	\$163,905	\$197,490	\$354,774
b. Cost of Goods Sold (COGS)	\$106,908	\$140,549	\$255,692
c. Gross Profit (Net Sales minus COGS) (calculated)	\$56,997	\$56,941	\$99,082
d. Interest Expense for the Year	\$18,489	\$50,236	\$89,833
e. Net Income after Tax	-\$43,539	-\$73,358	-\$98,932
STATEMENT OF CASH FLOWS			
a. Cash Flow provided by Operating Activities	-\$24,638	\$12,153	-\$1,681
b. Capital Expenditures (property, plant, equipment)	-\$10,033	-\$6,309	-\$4,960

ATTACHMENT K. FEDERAL AND OTHER STATE SPECIFICATIONS

The following provisions govern this product and the related technical requirements. Keep these in mind when preparing the Vendor's response

FNS HANDBOOK 901 PROVISIONS AND OTHER FEDERAL PROCUREMENT REQUIREMENTS

- a) No component or documentation of the Crossroads system will be in the public domain.
- b) Federal regulations 2 CFR § 200.315 provides for title to intangible property acquired under a Federal award. This regulation is located at the following website <https://www.ecfr.gov> .

The regulation includes that FNS reserves a royalty-free, nonexclusive, and irrevocable license to reproduce, publish, or otherwise use and to authorize others to use for Federal government purposes, the North Carolina Crossroads software and modifications thereof, and associated documentation designed, developed, or installed with Federal financial participation.
- c) Federal regulations 2 CFR § 200.317 (Procurement by states). This regulation is located at the following website <https://www.ecfr.gov> , and includes a list of provisions under 2 CFR 200 Appendix II that must be included in this RFP.
- d) Federal regulations 2 CFR Part 416 (Special Procurement Provisions). This regulation is located at the following website <https://www.ecfr.gov> , and includes exclusions on prospective contractors that also develop procurement documentation related to this RFP.
- e) Federal regulations 2 CFR § 421.10 (Drug-Free Workplace Act). This regulation is located at the following website <https://www.ecfr.gov> , and includes USDA policies and procedures for compliance with the Act.
- f) Federal regulations 28 CFR Part 35 (Americans with Disabilities Act). This regulation is located at the following website <https://www.ecfr.gov> , and implements Subtitle A of Title II of the Americans with Disabilities Act.

FNS APPROVAL

- a) This Crossroads RFP and resulting Contract is dependent upon FNS approval. Delays in approval may impact the timeline and schedule for Contract execution.

COMPLY WITH STATE CIO / DIT / ITD REQUESTS FOR ADDITIONAL SUPPORT

- a) If requested by the State, the Vendor will be required to support, at no additional cost, product reviews and assessments, various risk management, problem or issue resolution or other requests regarding WIC Crossroads from the State Chief Information Officer (CIO), the Department of Information Technology (DIT), and the DHHS Information Technology Division (ITD).
- b) In the event the State of North Carolina declares an emergency or disaster at the county, geographic region, or statewide level, the Vendor will assist the State as requested in restoring the State production system or implementing any emergency software modifications needed to minimize impact to participants of Crossroads programs.

VENDOR SITE VISITS

- a) The State's designated representative(s) and/or FNS may visit the Vendor's site(s) at any time with twenty-four (24) hour notice.

COMPLIANCE WITH STANDARDS, OPERATIONAL SPECIFICATIONS, AND FNS REQUIREMENTS

- a) Crossroads will remain compliant with the most recent version of the following standards and specifications
 - Software development best practices and standards such as the Agile methodology.
 - The FNS Operating Rules for WIC EBT systems as defined by USDA/FNS.
 - The FNS Technical Implementation Guide (TIG)
 - The FNS WIC Universal MIS-EBT Interface (WUMEI)
 - The NC Technical Architecture System Design (TASD)
 - The FNS Handbook 901
- b) Each major release of Crossroads will contain a mutually agreed number of Change Request hours, and a mutually agreed number of defect corrections, for the Vendor to meet the SLA.
- c) Vendor will furnish the necessary staff, material, travel expenses, software licenses, digital certificates, equipment, services, and facilities to perform the work described in this RFP. The State's designee(s), including auditors, and/or FNS may visit the Vendor's site(s) as stipulated under Attachment K.
- d) All Vendor / sub-contractor staff (including but not limited to software development, build, test, installation, help desk, product management, etc.), facilities, and equipment including all databases, servers and workstations (such as environments for software development, build, test, etc.) and tools (such as FTP storage sites, cloud hosting sites, issue reporting systems, etc.) will be physically located in the continental United States.

Only Vendor / sub-contractor staff physically located in the United States, including its territories, will administer equipment servers and tools.

b) Requirements and Specifications (Chapter 3 in RFP)

Voyatek has organized our offer per the RFP guidance in section 6.3 Instructions for Offer Submission, matching the section numbering within Requirements and Specifications of our offer to that of the RFP.

3.1 General Requirements and Specifications

3.1.1 REQUIREMENTS

Requirement means, as used herein, a function, feature, or performance that the system must provide. If the offer cannot meet the requirements, they will not be evaluated.

3.1.2 SPECIFICATIONS

Specification means, as used herein, a detailed description that documents the function and performance of a system or system component.

The apparent silence of the specifications as to any detail, or the apparent omission of detailed description concerning any point, shall be regarded as meaning that only the best commercial practice is to prevail and that only processes, configurations, materials and workmanship of the first quality may be used. Upon any notice of noncompliance provided by the State, Vendor shall supply proof of compliance with the specifications. Vendor must provide written notice of its intent to deliver alternate or substitute Services, products, goods or other Deliverables. Alternate or substitute Services, products, goods or Deliverables may be accepted or rejected in the sole discretion of the State; and any such alternates or substitutes must be accompanied by Vendor's certification and evidence satisfactory to the State that the function, characteristics, performance and endurance will be equal or superior to the original Deliverables specified.

3.1.3 SITE AND SYSTEM PREPARATION

Vendors shall provide the Purchasing State Agency complete site requirement specifications for the Deliverables, if any. These specifications shall ensure that the Deliverables to be installed or implemented shall operate properly and efficiently within the site and system environment. Any alterations or modification in site preparation, which are directly attributable to incomplete or erroneous specifications provided by the Vendor and which would involve additional expenses to the State, shall be made at the expense of the Vendor.

3.1.4 EQUIVALENT ITEMS

Whenever a material, article or piece of equipment is identified in the specification(s) by reference to a manufacturer's or Vendor's name, trade name, catalog number or similar identifier, it is intended to establish a standard for determining substantial conformity during evaluation, unless otherwise specifically stated as a brand specific requirement (no substitute items will be allowed). Any material, article or piece of equipment of other manufacturers or Vendors shall perform to the standard of the item named. Equivalent offers must be accompanied by sufficient descriptive literature and/or specifications to provide for detailed comparison.

3.1.5 ENTERPRISE LICENSING

In offering the best value to the State, Vendors are encouraged to leverage the State's existing resources and license agreements, which can be viewed here:

<https://it.nc.gov/resources/statewide-it-procurement/statewide-it-contracts>

- a) Identify components or products that are needed for your solution that may not be available with the State's existing license agreement.*
- b) Identify and explain any components that are missing from the State's existing license agreement.*
- c) If the Vendor can provide a more cost-effective licensing agreement, please explain in detail the agreement and how it would benefit the State.*

Voyatek has reviewed the General Requirements and Specifications sections of the RFP. We understand and acknowledge how the State has defined requirements and specifications. Voyatek endeavors to use the best commercial practices in system maintenance and enhancement (M&E) services for the WIC systems we support, including the Crossroads WIC MIS for North Carolina. For the next contract for system support for NC WIC, Voyatek will comply with all system specifications and utilize innovative and efficient practices in our support of the Crossroads WIC MIS. Our experience with the system and our continual adherence to best practices will provide North Carolina with continued high-quality support.

For deliverables that are related to site or system preparation, Voyatek will provide NC WIC with complete site requirement specifications so that the requirements or obligations of the State are clear to the State. Such requirements will be minimal as we transition to the cloud-hosted platform. We understand that any alterations or modifications in site preparation due to incomplete or inaccurate specifications provided by the Voyatek team which result in additional State expenses shall be made at Voyatek expense.

For hardware or software required for the Crossroads WIC MIS system performance, operation, or support, Voyatek understands that, if equivalent software or hardware is suggested by Voyatek from time to time, it is our obligation to explain to NC WIC why we are suggesting a change and why such a change is in the best interest of the State. A key area where such suggestions will be made is in the rehosting transition from the NC Data Center to the cloud.

We have reviewed the State's statewide IT contracts published at this link in the RFP (<https://it.nc.gov/resources/statewide-it-procurement/statewide-it-contracts>). We appreciate that the State has made bidders aware of the availability of such IT resources to provide NC WIC with optimized value pricing. At this time, given that the State is already hosting the Crossroads WIC MIS, Voyatek does not have any recommendations to make for the current platform and configuration. However, as described in [Appendix E: Rehosting Implementation and Rollout Plan](#), we will confirm with the State licensing requirements that might be able to take advantage of current State contracts with IT vendors. Additionally, where appropriate, identify any alternative product or license that may save the State money over the current IT contracts, we will bring these options to the attention of the State for consideration.

3.2 Security Specifications

Solutions Not Hosted on State Infrastructure

The Crossroads WIC MIS will be required to receive and securely manage data that is classified as Restricted. Refer to the North Carolina Statewide Data Classification and Handling policy for more information regarding data classification. The policy is located at the following website: <https://it.nc.gov/document/statewide-data-classification-and-handling-policy>.

To comply with the State's Security Standards and Policies, State agencies are required to perform annual security/risk assessments on their information systems using NIST 800-53 controls. This requirement additionally applies to all Vendor-provided, agency-managed Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) solutions which will handle data classified as Medium Risk (Restricted) or High Risk (Highly Restricted) data.

Voyatek provides numerous hosting solutions for state information management systems that house data classified as Restricted and Highly Restricted including the management of WIC, Nutrition, Criminal Information, and Tax solutions. Voyatek currently provides a SaaS solution to the North Carolina Child and Adult Care Food Program and has completed the required controls for similarly classified data. The proposed team has experience working with North Carolina technology staff to complete the required documentation and readiness assessment activities.

The proposed Crossroads WIC hosting solution will be maintained within our Microsoft Azure Nutrition hosting environment and managed by Voyatek's Information Technology Services & Security team. Voyatek maintains an annual SOC 2 Type 2 audit and related procedures in support of both the hosting and software development activities for our Nutrition customers including North Carolina WIC. This process includes security and risk assessments designed to be consistent with NIST 800-53 controls.

Vendor Readiness Assessment Report

(a) Vendors shall provide a completed Vendor Readiness Assessment Report Non-State Hosted Solutions ("VRAR") at offer submission. This report is located at the following website: <https://it.nc.gov/documents/vendor-readiness-assessment-report>

Voyatek is providing a completed VRAR for the hosting of the Crossroads WIC system. The VRAR is specific to the architecture and hosting model needed to support the Crossroads system. Voyatek currently has an approved VRAR for the NC Connects CACFP system and the provided Crossroads VRAR shares many of the general security and hosting controls. Voyatek anticipates that approval of the final VRAR will be relatively quick given the shared nature of the hosting models. Refer to section [c\) Security Vendor Readiness Assessment Report \(VRAR\)](#).

Vendor 3rd Party Readiness Assessment Report

(b) Upon request, Vendors shall provide a current independent 3rd party assessment report in accordance with the following subparagraphs (i)-(iii) prior to contract award. However, Vendors are encouraged to provide a current independent 3rd party assessment report in accordance with subparagraphs (i)-(iii) at the time of offer submission.

(i) Federal Risk and Authorization Management Program (FedRAMP) certification, SOC 2 Type 2, ISO 27001, or HITRUST are the preferred assessment reports for any Vendor solutions which will handle data classified as Medium Risk (Restricted) or High Risk (Highly Restricted).

(ii) Reserved.

(iii) An IaaS vendor cannot provide a certification or assessment report for a SaaS provider UNLESS permitted by the terms of a written agreement between the two vendors and the scope of the IaaS certification or assessment report clearly includes the SaaS solution.

Voyatek maintains an annual SOC 2 Type 2 audit covering Security, Availability, Processing Integrity, and Confidentiality trust principles. This audit covers all WIC and Nutrition hosting environments along with their related software development and support activities. A copy of the most recent annual audit has been provided. The hosting of the North Carolina Crossroads system will be added to the scope of the audit and will be included in future audit periods.

Voyatek is proposing to utilize the Microsoft Azure Commercial Cloud for hosting the North Carolina Crossroads system. The Azure Commercial Cloud and all proposed PaaS services are FedRAMP High certified.

[Azure and other Microsoft cloud services compliance scope - Azure Government | Microsoft Learn](#)

Additional Security Documentation

(c) Additional Security Documentation. Prior to contract award, the State may in its discretion require the Vendor to provide additional security documentation, including but not limited to vulnerability assessment reports and penetration test reports. The awarded Vendor and any subcontractors of the awarded Vendor shall provide such additional security documentation upon request by the State during the term of the contract.

Voyatek currently supports both state-initiated and internal vulnerability tests for the Crossroads system. Voyatek's Information Technology Services & Security team uses real-time tools to detect environment vulnerabilities and to facilitate appropriate patching in development and production hosting environments. Voyatek performs penetration tests of corporate environments annually and can support environment-specific third-party tests of NC Crossroads environments as requested by North Carolina as part of our hosting services. Please refer to [Appendix Q: SOC 2](#) (System and Organization Controls 2) report for the period of March 1, 2023 – February 29, 2024. Pricing has been provided under optional services for a penetration test dedicated to the North Carolina hosting infrastructure.

3.3 Enterprise Specifications

The proposed solution must externalize identity and access management. The protocols describing the State's Identity and Access Management can be found at the following link: <https://it.nc.gov/services/vendor-engagement-resources#Tab-IdentityAccessManagement-1241>

Describe how your solution supports the above protocols, as well as making them available for application integration/consumption.

Crossroads is integrated with the state's NCID identity management system. The system currently uses a web services integration with NCID; Voyatek has experience with this method as well as

SAML integration (used in the NC Connects CACFP application and the current Crossroads participant portal). The Crossroads team has been involved with and supported all recent upgrades to NCID services and uses automated methods to deploy configuration changes related to NCID to both pre-production and production environments. Voyatek anticipates transitioning the Crossroads system to utilize the NCID SAML protocol within the next several months.

Vendors should refer to the Vendor Resources Page for information on North Carolina Department of Information Technology regarding architecture, security, strategy, data, digital, identity and access management and other general information on doing business with state IT process.

The Vendor Resources Page found at the following link: <https://it.nc.gov/vendor-engagement-resources>. This site provides vendors with statewide information and links referenced throughout the RFP document. Agencies may request additional information.

Voyatek has reviewed North Carolina's current IT security standards and has extensive experience working with these standards. As part of the transition-in process, Voyatek will provide an updated security and vulnerability plan that provides a cross-reference between NC State security controls and requirements to Voyatek's internal policies and procedures along with related SOC 2 controls.

Voyatek staff are familiar with the updated standard for maintaining Network Architecture and Technology Stack Diagrams using the provided Visio templates. Voyatek currently maintains these diagrams for the CACFP Connects system and hosting environment. As part of transition in, Voyatek will provide the required diagrams for NC review and approval. Based on Voyatek's experience working with North Carolina IT staff, we anticipate streamlined approval of the required documentation approval.

Preliminary versions of these diagrams have been provided within the attached completed Vendor Readiness Assessment Report and within the Architectural Diagrams section of this document. These diagrams were prepared based on Voyatek's proposed hosting solution and our understanding of the Crossroads system.

3.4 Business and Technical Requirements

This RFP seeks to obtain a Vendor to provide maintenance and enhancement services of the North Carolina Crossroads WIC Management Information System, including system cloud hosting, in accordance with the Service Level Agreement and other technical specifications. Vendor must address each requirement listed within this Section 3.4 within their proposal to confirm that the proposed solution meets the requirements within this RFP.

As the vendor currently supporting the NC Crossroads WIC MIS, Voyatek welcomes the opportunity to compete for the State's ongoing system support business again. In the following sections, we provide our qualifications and understanding of the State's business and technical

requirements, including transitioning the system hosting to the cloud, in accordance with the service level agreement and other technical specifications.

3.4.1 System

- a) Confirm that the State will retain all ownership rights to the Crossroads source code and its derivative works.*
- b) The State will not consider offers for an alternative replacement MIS system, nor consider offers to convert the State's Crossroads ownership rights to a Software as a Service (SaaS) solution. Confirm that Vendor solution is not an alternate replacement MIS system and that Vendor will not convert Crossroads ownership rights to a SaaS solution.*
- c) Confirm that Vendor will not impose any "black out periods" on any M&E activity, nor allow Vendor efforts with other state agencies to introduce delays or other impacts on execution of this contract.*

Voyatek understands and confirms that the State will retain all ownership rights to the Crossroads source code and its derivative works. In our long history of supporting WIC MIS systems, Voyatek has been the custodian, not the owner of those systems. We developed our first WIC MIS for Maryland over twenty years ago as a government-owned system and through all the transfers of that system to other state agencies, we have always understood and adhered to the intellectual property rights of the state agency governments to their systems. Likewise, for our other Crossroads WIC MIS support contracts, we understand and support that the respective state agencies own those versions of Crossroads.

Voyatek is proposing to support the NC Crossroads WIC MIS in a manner consistent with the requirements of the RFP and in alignment with North Carolina's expectations. We are not proposing an alternative WIC MIS nor are we proposing to convert the State's system to a software as a service (SaaS) solution. We are offering only to provide ongoing support that meets the State's and NC WIC's requirements in the same high-quality fashion that NC WIC has come to expect from us.

Voyatek confirms that we will not impose any "blackout periods" on any M&E activity throughout the life of the contract nor allow our other WIC MIS support contracts with other state agencies to introduce delays or other negative impacts on our support for NC WIC. We are proud of our approach to maintaining the independence of each of our WIC support teams by providing support via dedicated teams focused on each respective client. However, we do continuously seek to provide continuous improvement to each WIC client via the sharing of ideas, designs, and features across our WIC Practice. This sharing is encouraged via a weekly meeting of our WIC project managers as well as dialog between our technical leads and has often led to significant cost savings for WIC clients because of the work done for another WIC client by a different team. Voyatek offers the same potential to NC WIC.

3.4.2 Other Maintenance Tasks

The following requirements govern this product and the related technical specifications. Vendor will indicate compliance with each requirement within Table 3.4.2 located below.

As shown in the table below, Voyatek complies with all the requirements associated with Other Maintenance Tasks.

Table 1: Other Maintenance Tasks

Does the Vendor meet the requirements listed below?	Yes	No
a) Interface with Existing or Future WIC Electronic Benefits Transfer (WIC EBT)	X	
b) Correction of Unknown Defects or Issues Introduced Prior To Contract Execution	X	
c) Maintenance Change Requests and Data Corrections	X	
d) Other USDA Food and Nutrition Service (FNS) Programs covered by this RFP	X	

Interface with Existing or Future WIC Electronic Benefits Transfer (WIC EBT)

Crossroads is required to interface with the current or any future WIC EBT provider. As of the date of this RFP, the Crossroads system is only compatible with the interim version of the WIC Universal MIS-EBT Interface (WUMEI) from July 2013. The system is scheduled for an upgrade to support the latest WUMEI by March 2026.

1. Should the upgrade to the latest WUMEI specification not be completed prior to the March 2026 deadline, planning will commence by the State, the WIC EBT Provider, and the Vendor to complete the upgrade the Crossroads production system to the new WUMEI as well as any related technology changes at no additional cost. All planning, JAD sessions, development, testing, support for UAT, pilot and rollout related to the WUMEI will be performed by the Vendor. The production upgrade completion date will be solely determined by the State.

2. Should Crossroads contain an interface to a non-State owned or licensed software component required to support the WUMEI interface, the Vendor must maintain or substitute such component to ensure no interruption in EBT processing.

Voyatek actively collaborates and supports interfaces with all three current WIC-based EBT vendors: CDP/FIS, Conduent, and Solutran (exiting the WIC market). Across the state agencies that we support, we have extensive experience managing online EBT interfaces, ranging from WUMEI versions 2012 to 2020, and we have established robust processes for operating and monitoring both real-time and batch EBT interfaces.

FNS sought out Voyatek personnel for our input while they worked to develop the latest WIC Universal MIS-EBT Interface (WUMEI) 2022 standard. Over the last five years we have

participated in monthly technical review sessions working on interface standardization. Voyatek was the first WIC MIS vendor to implement the 2020 JSON-based universal interface. We have successfully implemented the latest CDP interface in both California and Florida. This interface is closest to the 2022 interface standard and would be available to North Carolina. In addition, Voyatek has been selected for a significant modernization project to collaborate with CDP in developing a universal WUMEI API layer. This effort is described in more detail in [3.5.4 Coordination with WIC EBT Provider / Interface with the EBT System](#). This would be another option for North Carolina to consider as the new 2022 API will be completed in advance of the State's scheduled upgrade deadline of March 2026.

If the State has not completed the upgrade to the latest version of the WUMEI prior to the start of the new contract, Voyatek will work with the State and the EBT Provider to complete the upgrade as well as related technology changes at no additional cost. We will lead the requisite planning and JAD sessions, perform associated development and testing, and support the implementation of the new WUMEI in close coordination with NC WIC and the EBT Provider. We will also support non-State-owned or licensed software component required to support the current WUMEI interface without disruption to EBT processing.

Voyatek is also preparing a more comprehensive modernization to expand EBT scope and to transition to new web technologies. This includes upgrades to administrative functions and reporting capabilities. This upgrade path is available but elements beyond the EBT upgrade scope would need to fall under the change request process.

Correction of Unknown Defects or Issues Introduced Prior To Contract Execution

Vendor must correct any unknown defects or issues in the Crossroads system that originated prior to work by the Awarded Vendor, using the defect correction process and at no additional cost to the State. All defects known prior to the award of this Contract will be classified as adaptive changes and addressed by the Awarded Vendor using the Maintenance Change Request process.

Voyatek understands that all defects known before the start of the new contract will be classified as adaptive changes under the new contract which we will then address using the Maintenance Change Request process. As the incumbent vendor, we strive to continually minimize the backlog and we will strive to transfer no known defects into the new contract. In addition, we understand and accept that all unknown defects or issues in the system at transition to the new contract, when identified in the future, will be addressed via the defect correction process at no additional cost to the State.

Maintenance Change Requests and Data Corrections

The Vendor must perform all application maintenance, which refers to routine support activities that include corrective, adaptive, and perfective changes.

1. *Corrective changes are tasks to correct errors or deficiencies in the Crossroads system, at no additional cost to the State;*

2. *Adaptive changes are revisions to the Crossroads system to meet the changing WIC, State Agency, or USDA/FNS policy, statutory, security, or regulatory requirements, and will use the change management process and Supplemental Service Hours;*

3. *Perfective changes are improvements to the Crossroads system so that it will perform in a more efficient, economical, and/or effective manner, at no additional cost to the State*

Corrective and perfective application maintenance examples can include activities such as revising standard or state-created ad-hoc reports, creating new reports or data extracts (CSV or similar formats at the sole discretion of the State), creating (and executing at the request of the State) data scripts to implement limited data correction changes regardless of root cause, and making limited performance alterations or minor improvements to imbedded passwords, data input and display screen designs and layouts.

State personnel will also be granted read-only access to the cloud computing platforms at no additional cost, to exercise data reporting, or other queries against the Production and non-Production environments at the sole discretion of the State.

Voyatek understands the definition and examples of corrective, adaptive, and perfective changes. Corrective and perfective changes will continue to be made to the system by Voyatek at no additional cost to the State while adaptive changes will be made only when approved by the State via the change management process and utilizing Supplemental Service Hours to perform the associated work. Voyatek will continue providing and managing the different types of changes in coordination with the NC Crossroads WIC MIS Release Manager.

In support of these types of changes and following the rehosting transition, State personnel will be granted read-only access to the cloud computing platforms at no additional cost so that they can perform data reporting / queries against both Production and Non-Production environments as needed. As part of the transition to the cloud, Voyatek will work with the State personnel to provide orientation and training to the cloud environments and demonstrate the techniques to perform independent queries and analysis.

Voyatek can support NC staff access to the Crossroads read-only environment using one of two methods:

- Users can log into a cloud environment to allow local execution of SQL queries to the production replica. The proposed Azure SQL Managed Instance will utilize Microsoft's Business Critical service tier. This tier maintains three separate servers to support immediate failover of the production environment. One of these environments also allows real-time access to a read-only production replica. NC staff can use this read-only environment to get access to current production data.
- Alternatively, NC and Voyatek can create a VPN tunnel to the hosting environment to allow authorized staff to develop and maintain queries against the Crossroads database.

Other FNS Programs Covered by this RFP

The Farmers' Market Nutrition Program (FMNP) and the Breastfeeding Peer Counseling Program (BFPC) functionality are also components of the North Carolina Crossroads system and are covered by all M&E processes throughout this RFP.

As part of the new contract, Voyatek will continue supporting the North Carolina Farmers' Market Nutrition Program (FMNP) and the Breastfeeding Peer Counseling Program (BFPC) functionality in the NC Crossroads WIC MIS. While these are separate programs, their associated system functionality is tightly integrated within the Crossroads WIC MIS. As such, we will continue to support them as part of normal change, release, and defect management for the rest of the system.

3.4.3 Product Deliverables

a) The Vendor's proposed schedule for the provision of product deliverables and documentation for review and approval by North Carolina WIC must adhere to the dates specified in Table 1 below. Electronic copies of the draft and final documentation and deliverables will be supplied to the State through use of a secure electronic documentation repository, hosted and managed by the Vendor. Electronic copies will be provided in Microsoft Office 365 format, unless otherwise specified within this solicitation.

Voyatek acknowledges that the delivery of product deliverables and documentation to NC WIC will adhere to the dates specified in the RFP's Table 1 – List of Product Deliverables which is replicated in [Table 2](#) below. We will continue to use SharePoint as our secure electronic documentation repository. SharePoint will support the organization of our work products and deliverables as well as delivery of deliverables for State review and approval. SharePoint provides complete version management including date and time of any changes as well as who made each change to a deliverable. Customers can set alerts to be notified by SharePoint of document updates as desired and can receive those alerts as changes are made or in periodic digests. These electronic files will continue to be provided in Microsoft Office 365 format for ease of review and use by the NC WIC team.

b) State comments will be provided to the Vendor within ten (10) Business Days of the receipt of draft deliverables. Within five (5) Business Days of receipt of State comments, and after incorporating such comments, the draft of the documentation will be delivered to the State. The State desires to keep deliverable review and revision cycles to a minimum. The above process will be repeated until the State has approved the deliverable in writing. Acceptance by the State will be in the form of a written acknowledgement that the deliverable meets the specifications as specified in this RFP.

Voyatek acknowledges and appreciates that State comments will be provided to us within ten business days of receipt of each draft deliverable. Following receipt of State comments, we will modify each deliverable, as necessary. A new version of the deliverable will be submitted to the state within five business days of receipt of the State's comments. If necessary, we will repeat

the process until the State is satisfied with the content and quality of the deliverable, though we strive to limit the need to review a deliverable to a single pass out of respect for stakeholders' time. Sometimes, as it makes sense, we will schedule and conduct a walkthrough of a deliverable if there are significant comments or indication of misunderstanding of the intent or structure of one of our deliverables. We will not consider a deliverable final and approved until we receive written confirmation of acceptance by the State in writing.

c) The Vendor will update and maintain product deliverables and documentation for the duration of the Contract, at no additional cost to the State. The approved deliverables and documentation will be updated to reflect changes in system design or operations or as requested by the State. The timing for product deliverables and documentation updates will be determined as part of each change request and each major release.

Deliverables requiring periodic updates will be submitted per the document update schedules included in the description of each deliverable in the associated sections of this RFP.

Voyatek updates and maintains product deliverables and documentation for the duration of our contracts via our SharePoint project sites at no additional cost to customers. This is part of our standard project management procedure. We will retain the draft versions until written acceptance of each deliverable at which point the final approved deliverable will be moved to the Approved Deliverables area for reference throughout the project.

In addition, our project and product management deliverables are updated as needed following initial acceptance to keep them consistent with ongoing project decisions and processes or product scope and features changes. With each project change request, we will assess the impact of the change on project and product deliverables and inform the State as part of our documentation of the change request impact. As those change requests are then completed and delivered in system release(s), the affected documentation will also be delivered concurrent with the release code and the associated Release Notes will detail the documentation changes made.

For deliverables that require periodic updates (e.g., status reports), the updates will be provided on the agreed upon schedule and in the manner preferred by the State as discussed and agreed at the project kickoff. The SharePoint repository will house the recurring deliverables in an accessible structure so that the archive is available throughout the contract for reference as needed.

d) Timelines for the submission of deliverables are provided in Table 1 below. Details as to what will be in each deliverable are provided in subsequent sections. The Vendor will submit the following deliverables within the timeframe listed for each deliverable in Table 1, or as otherwise specified in this RFP. If preferred, the Vendor may include each of these deliverables in the Appendices section of its proposal bid (after Attachments) and will label each of the deliverables that are requested with the bid proposal as indicated in the "RFP Response Deliverable Label" column in Table 1. These appendices are the agency's preference, but not a requirement.

Voyatek acknowledges and agrees to the timeline for deliverables as noted in Table 1 of the RFP. For clarity, we have reproduced the table below, though it is numbered as [Table 2](#) in our proposal.

As a part of our proposal, **we are including the requested deliverables as appendices to our proposal**. These plans are vital to helping North Carolina understand our proposed approach to managing the project and continuing to provide excellent support for the NC Crossroads WIC MIS. Therefore, we felt it was important to submit draft versions of the deliverables as part of our proposal. Upon project initiation, the Voyatek product manager will oversee the updating and submittal of the final versions of each deliverable as well as managing the maintenance of approved deliverables throughout the contract as described above.

e) Deliverables must be itemized under Attachment D in order to receive payment. Deliverables not itemized under Attachment D are at no additional cost.

Voyatek acknowledges that deliverables not itemized under Attachment D – Cost Form will be provided at no additional cost to the State.

Table 2: RFP Table 1 List of Product Deliverables

ID	Deliverable Name	Deliverable Timeline	RFP Response Label
1	Transition-In Plan	Described in bid response proposal	Appendix A: Transition-In Plan
2	Product Management Plan	Described in bid response proposal	Appendix B: Product Management Plan
3A	Product Work Plan and Schedule DRAFT	Described in bid response proposal	Appendix C: Product Work Plan and Schedule
3B	Product Work Plan and Schedule FINAL	During Transition-In – 45 Calendar Days after Contract execution date	
4	Quality Assurance Management Plan	Described in bid response proposal	Appendix D: Quality Assurance Management Plan
5	Communication and Coordination Plan	Described in bid response proposal	Appendix P: Communication and Coordination Plan
6	Maintenance and Enhancement Status Reports	Monthly during the life of the contract, aligned with monthly invoice	
7	UAT Readiness Reports	14 Calendar Days Prior to each UAT Start	

ID	Deliverable Name	Deliverable Timeline	RFP Response Label
8	UAT Completion Reports and System Documentation	21 Calendar Days prior to each Deployment	
9	Production Deployment Plan	During Transition-In: 90 Calendar Days prior to the first statewide deployment	
10	Disaster Recovery and Contingency Plan	Described in bid response proposal	Appendix F: Disaster Recovery and Contingency Plan
11	Security and Vulnerability Plan	Described in bid response proposal	Appendix G: Security and Vulnerability Plan
12	Risks and Issues Management Plan	Described in bid response proposal	Appendix H: Risks and Issues Management Plan
13	Configuration Management / Release Management Plan	Described in bid response proposal	Appendix J: Configuration Management / Release Management Plan
14	Evidence of Vendor and financial stability (See Section 7 for acceptable documentation)	Described in bid response proposal	Appendix K: Evidence of Vendor Financial Stability
15	Transition-Out Plan	Described in bid response proposal	Appendix L: Transition-Out Plan
16	Transition-Out Completion Report	During Transition-Out: 10 Calendar Days prior to Contract termination or expiration	
17	Partnerships and Contractual Relationships	Described in bid response proposal	Appendix M: Partnerships and Contractual Relationships
18	Risk and Security Assessment of Vendor critical systems and infrastructure	Assessment due during the Transition-In Phase.	
19	Help Desk Plan	Described in bid response proposal	Appendix N: Help Desk Plan

ID	Deliverable Name	Deliverable Timeline	RFP Response Label
20	Rehosting Implementation and Rollout Plan	Described in bid response proposal	Appendix E: Rehosting Implementation and Rollout Plan
21	Vendor-Hosting Status Report	Monthly during the life of the contract, aligned with monthly invoice	

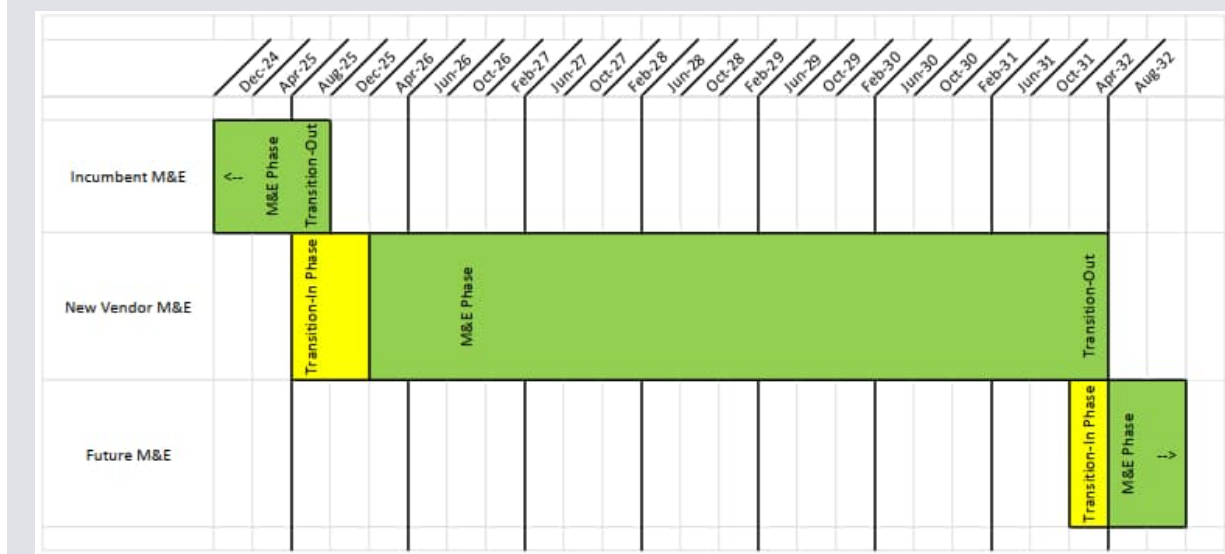
3.5 Business and Technical Specifications

Please describe your proposed approach to meet all specifications, including capabilities, features, and limitations. All pricing and cost information will be restricted to the Pricing Section of the Vendor's response.

In the following subsections of 3.5 Business and Technical Specifications, Voyatek has adhered to the RFP numbering as requested, detailing our proposed approach in each section. In addition, we have provided the requested or suggested plans as appendices.

3.5.1 Scope

The scope of this RFP includes two phases, the Transition-In Phase and the Maintenance and Enhancement Phase, as illustrated here with tentative dates that are subject to change.



a) Phase I: Transition-In Phase

Using the parameters below, describe Vendor's approach to implement the transition-in phase:

1. *Expected Phase Timeframe: eight (8) months in duration after Contract Execution.*
2. *The Transition-In Phase is expected to begin immediately after Contract award) and last until either the Maintenance and Enhancement Phase begins or until the existing contract with the incumbent vendor ends. ("Transition-In Phase End Event"), whichever Transition-In Phase End Event occurs first.*
3. *At the initiation of the Transition-In Phase, the Vendor and the State should meet during the Kick-Off Meeting to discuss and prepare for the completion of Transition-In Phase tasks.*
4. *Vendor should include a Monthly Transition-In Phase Fee for performing the Transition-In Phase tasks outlined in this RFP.*

At the beginning of the new contract, the Voyatek product manager will work with NC WIC to schedule and conduct a Kick-Off Meeting to review the scope, deliverables, and schedule for the new contract and to identify key differences from the current M&E contract so that parties and stakeholders are clear on how the transition to the new contract will work. Following the Kick-Off Meeting, to confirm stakeholders are operating with the same understanding, the Voyatek product manager will summarize the decisions, issues, and action items from the meeting in a memorandum and submit it to the State for review and approval.

As shown in the chart above from the RFP, the 8-month Transition-In period is planned to commence on August 1, 2025, and extend through March 31, 2026, which is the end of Voyatek's current M&E contract. Based on the clarifications provided by the State during the RFP Questions & Answers period, our understanding is that all M&E support for the system running in the NC Data Center will be provided by Voyatek under our current contract. Upon execution of the new contract, we will begin the preparation for transitioning the system to the Azure cloud platform. These transition activities are described in [Appendix E: Rehosting Implementation and Rollout Plan](#). Voyatek acknowledges that NC has requested that the hosting environment migration be completed within the eight-month transition-in period. **However, Voyatek proposes completion of the transition in four (4) months with a final cutover date mutually agreed upon with NC WIC.** Upon cutover of the production Crossroads system to the Azure cloud, the Voyatek team will:

- ✓ Continue support of NC Crossroads with the M&E costs covered under our current contract.
- ✓ Commence hosting support for the new cloud platform under the new contract.
- ✓ Support the NC Data Center team as needed to complete the decommissioning of the data center platform as the final portion of the current contract.

At the end of the Transition-In Phase, as the current contract ends, our team will commence M&E services under the new contract for the Crossroads WIC MIS rehosted in the cloud.

Voyatek has included appropriate costs for Transition-In in Attachment D, Cost Form.

b) Phase II: Maintenance and Enhancement Phase

Following the Transition-In period, the core concept of the Contract is for the Vendor to provide development, UAT, deployment, and ongoing Help Desk support of multiple iterative releases of the Crossroads system over the life of the Contract as shown below.

During the Maintenance and Enhancement Phase, the Vendor is expected to provide full Maintenance and Enhancement Services support for Crossroads, independent of the incumbent vendor.

The Maintenance and Enhancement Phase is expected to start on the first Calendar Day after the Transition-In Phase End Event occurs. The Vendor will be expected to perform tasks and deliverables included under Scope of Work, Technical Specifications, and Attachment K.

The Voyatek team will commence the Maintenance and Enhancement (M&E) Phase of the contract at the completion of the Transition-In Phase. The Voyatek product manager will work with the Voyatek team to transition ongoing M&E of the Crossroads system to the workflow, release schedule, and processes as required and agreed during the Kick-Off Meeting based on the RFP's Scope of Work, Technical Specifications, and Attachment K (Federal and Other State Specifications).

1. Explain the Vendor's process, either an agile/waterfall hybrid for the State to receive a minimum of three (3) major releases per year, or an agile continuous delivery approach that aligns with the States' business needs and resources.

As the incumbent vendor supporting North Carolina's Crossroads system, Voyatek has consistently demonstrated flexibility in our approach to software releases, aligning with the State's evolving business needs and priorities. Voyatek takes pride in our adaptability, which sets us apart from other vendors.

Voyatek is committed to delivering a minimum of three major software releases per year. However, we strongly advocate for more frequent releases, as limiting updates to three per year may not provide enough opportunities to address emerging user needs and rapidly changing circumstances. In today's dynamic environment, the ability to respond quickly to new challenges and policy changes plays a crucial role in maintaining the efficiency and effectiveness of critical systems like the Crossroads MIS. We also recognize that unforeseen events can require deviations from established release plans. Government programs often need to adapt to external factors beyond their control, a prime example of which was the national formula shortage in 2022, which had a significant impact on WIC participants. The urgency of the situation required an immediate response, prompting both the state and Voyatek to adjust the planned release schedule. Voyatek collaborated closely with the state to implement critical changes to data, processes, and software functionality so affected families could continue accessing the necessary formula benefits without disruption. This experience highlights the importance of a flexible and responsive approach to software deployment.

Voyatek has fully embraced Agile methodologies across the various projects we support, including our work with North Carolina. Continuous improvements to both the development and deployment processes have increased efficiency, stability, and reliability. For instance, the introduction of Git and standardized code check-in practices with Azure DevOps has streamlined version control and collaboration among developers. Additionally, by fully automating software deployments using Octopus across multiple environments, we have eliminated manual errors, improved deployment consistency, and established a repeatable process that has strengthened our ability to deliver updates more frequently and reliably.

For the next NC Crossroads M&E contract, Voyatek proposes to continue to deliver system change management using an agile continuous delivery approach.

2. Describe the Vendor's approach in providing a minimum number of Change Requests and defect corrections, as provided by the State in each quarter. This approach will ensure that the business needs of the State across the clinic, retail vendor, financial, and related components of Crossroads are being addressed per quarter.

Voyatek will work closely with NC WIC to plan and deliver each system release with the requested and desired level of system changes (defects and/or change requests) to meet the needs of the North Carolina WIC program. We acknowledge and commit to the RFP requirements to maintain staff to correct a minimum of 30 defects and support 150 hours or more of approved change requests per quarter. Voyatek staff will also have the capacity to support 60 issues requiring assistance during each quarter. Having supported the NC Crossroads system for the past six years, we are keenly aware of the number of code fixes and issues that are encountered on a weekly, monthly, and quarterly basis. Based on our extensive experience in supporting North Carolina WIC, we have proposed project staffing to support these levels of anticipated system changes, backed up by our extensive WIC Practice which can supply additional on-demand resources as needed.

3. Explain how the Vendor maintains and trains appropriate development and test staff to address the breadth of clinic, retail vendor, financial, and related components potentially affected in each major release.

Voyatek has been managing WIC systems for over two decades and supports a wide range of WIC programs across the country. Our Nutrition/WIC Practice is comprised of approximately 80 staff supporting our WIC customers. This large pool of talent enables us to provide cross-team support as needed and to share ideas and features that are developed for one customer with other customers interested in the same or similar enhancements.

WIC is a complex program and Voyatek has built our team with care, establishing a balance between WIC experience, technical skills, and nutrition knowledge. The latter drove the decision to hire three registered dietitians and two former WIC local agency coordinators as part of the staff. Voyatek team members understand the essential business elements of WIC by conducting regular cross-training and providing a specialized WIC orientation for developers. Understanding

the business of WIC across the many aspects of the program that depend on the WIC MIS for support is vital for our teams to properly support our customers. This training provides a framework of understanding for the technical staff that enables them to better understand requirements and issues which, in turn, provides more efficient, cost effective, and accurate system modifications.

Voyatek builds teams mindfully to focus on their respective WIC clients, the system they support for each client, and the individual needs of each client. With any system maintenance and enhancement contract, what often sets us apart from other offerors is the depth of expertise in the personnel that we provide – a team that provides excellence, commitment, and outstanding service because of their extensive experience. An additional benefit of our large customer base is our ability to assign focused support teams to each project while, at the same time, maintaining sufficient resources to cross-train other team members or new hires so we can respond to the needs of our customers promptly and efficiently.

The proposed North Carolina Crossroads team has extensive experience working with Crossroads and North Carolina WIC. Most members of the team were involved in the original development of the Crossroads system and have experience working with North Carolina WIC policies and procedures. The Voyatek Crossroads team maximizes productivity due to a strong understanding of the Crossroads platform and North Carolina's history with the system.

4. Describe Vendor's Rehosting Implementation and Rollout Plan. (Note: If preferred, you may attach a Plan instead. An attached plan is the agency's preference, but not a requirement.) Include in this description, the Vendor's approach in rehosting the State hosted Crossroads solution to a Vendor managed cloud infrastructure prior to the start of the Maintenance and Enhancement phase and address details on the proposed 3rd party cloud computing provider, and the service model proposed between the Vendor and the cloud provider (IaaS, PaaS, etc.). Describe and explain the Vendor's approach to preserving and transferring control of the 3rd party cloud infrastructure to the State or its designee during Transition-Out.

The Rehosting Implementation and Rollout Plan outlines the strategy and technical approach for migrating the Crossroads environments from an on-premises North Carolina data center to a Voyatek-managed Azure tenant. This migration will encompass the UAT, Staging, Sandbox, Production, and Disaster Recovery environments.

The plan focuses on leveraging Azure East US Commercial Cloud through a strategic combination of Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS) solutions. The web and application tiers will undergo a lift-and-shift migration, while Azure-native services will be used for databases, storage, and networking to enhance performance, scalability, and manageability.

Voyatek's approach prioritizes simplification and automation, utilizing native Azure services wherever possible. Industry-standard automation tools like Terraform and Octopus will be used to deploy both infrastructure and applications, creating a flexible, cost-efficient, and future-ready cloud environment. Instead of relying on the Azure Migration Tool, which can carry over legacy

configurations, technical debt, and inefficiencies, Voyatek will build fresh environments. This approach enables an optimized, secure, and scalable deployment aligned with Azure best practices.

As part of the migration process, Voyatek will collaborate with NC DIT to review the existing infrastructure, document detailed configurations, and identify dependencies or constraints that could impact the transition. These discussions will provide a complete understanding of the current state.

Although the RFP permits an eight-month hosting transition, Voyatek is confident in completing the process within four months. This confidence stems from Voyatek's recent successful transition of hosting for the Rhode Island Crossroads system. Over the four months of transition-in, Voyatek will:

1. Build out the new environments within a Voyatek-owned Azure tenant.
2. Document the detailed design of the environment.
3. Update existing plans that reference hosting infrastructure to maintain accurate documentation.

[Appendix E: Rehosting Implementation and Rollout Plan](#) provides a detailed roadmap for executing the migration, including step-by-step guidance for server and data transfers.

If North Carolina selects a different vendor for the next contracting period, as part of the transition-out process, Voyatek agrees to provide the following artifacts:

- Updated plans reflecting any modifications made during the hosting transition.
- Terraform scripts that are used to provision the Azure environment.
- Octopus deployment scripts for application code deployment.
- A copy of the latest production database and any production files stored in the environment at the time of transition.

Please see [Appendix E: Rehosting Implementation and Rollout Plan](#). Voyatek has included this optional draft plan to provide substantial detail on how we will approach the rehosting of the NC Crossroads WIC MIS to a cloud platform.

c) Transition-Out Period

Using the parameters below, describe Vendor's approach to implement the transition-out phase:

1. Expected Phase Timeframe: No more than four (4) months in duration, unless the Maintenance and Enhancement Phase is extended.

2. The State will initiate the Transition-Out Period during the Maintenance and Enhancement Phase by notifying the Vendor in writing to begin performing Transition-Out Period tasks.

3. The Transition-Out Period will end when the Vendor's Transition-Out Completion Report has been accepted by the State, or when the end date of the Contract has been reached.

The most important element in the transition of support for any system is the coordination and collaboration between the incoming and outgoing contractors. **This cooperation is vital to the success of the incoming contractor.** Voyatek understands the need for a smooth transition between service providers to avoid interruption of service to NC WIC or the participants. In the event we are not chosen as the subsequent M&E service provider, we will support a smooth transition to a new M&E provider. We understand that the State's intent is to accomplish that transition between service providers in no more than four months.

Upon notification by the State to commence Transition-Out, we will work with the State team to update and refine our Transition-Out Plan (delivered in draft with our proposal as [Appendix L: Transition-Out Plan](#)) based on which entity will be assuming M&E responsibility for the NC Crossroads WIC MIS. The Voyatek Transition-Out Plan details the process and activities necessary to transfer the Crossroads source code, system documentation, and system support artifacts into the incoming contractor's infrastructure and to provide complete knowledge transfer to prepare the incoming contractor for ongoing maintenance and enhancement of Crossroads. The following are the key elements of the transition:

- **Documentation:** Voyatek will transfer to the incoming contractor relevant, up-to-date system documentation (including, but not limited to DFDDs, data models, and the data dictionary), tools and utilities which are the property of the State, release notes, system operations process documentation, and system maintenance standards documentation. Voyatek will also provide an export of action items and finalized change request documents, including sample documents and templates used for the Change Request Process.
- **Repositories:** Voyatek will export from DevOps the defect tracking information (open and closed defects) and information on the SharePoint collaboration site in a format agreed to with the incoming contractor so that the information can be imported into their equivalent toolset. Emails related to open items will also be provided if not documented within the defect or enhancement. Voyatek will maintain the SharePoint collaboration site to allow State staff to download artifacts until the end of the contract / transition period.
- **System Code:** Voyatek will deliver the current and prior two major releases of the system source code, third-party libraries, applications, tools, and documentation necessary to compile, install and run the Crossroads software. In addition, an export of regression and

performance test artifacts, including test scripts, test cases, and test scenarios will be provided.

- **Knowledge Transfer:** Voyatek will conduct documentation reviews and virtual walkthroughs of system modules, batch processes, defect management techniques, system build and release processes, and system installation and configuration methods. During these meetings, Voyatek will review known system errors and documented workarounds, will lead hands-on system design and code walkthroughs, and will conduct open sessions as needed to address questions for the incoming contractor and NC WIC.
- **Work-in-Progress:** For enhancements and defects currently in development at the time of transition, Voyatek will provide recommendations for transitioning this work-in-progress and will coordinate with the incoming contractor to confirm that the new team understands the status of the design, development, and/or testing processes.

At the end of the transition period, Voyatek will provide a Transition-Out Completion Report which will document the activities conducted and Voyatek's assessment of the success of the transition. In addition, Voyatek will return system peripherals and other hardware and/or software owned by NC WIC.

3.5.2 Objectives

Transition-In Services

a) Describe how Vendor will provide "Transition-in" services, including:

- 1. The rehosting (or "lift and shift") of the WIC Crossroads applications and all data (including file system contents) to a Vendor managed cloud infrastructure*
- 2. Maintaining or substituting any non-State software components required to support WIC Electronic Benefits Transfer (EBT) processing*

Voyatek has long experience with maintaining the system in North Carolina. We were proud to successfully complete the last transition-in work in 2019, and we have necessary plans in place for how to accomplish the next transition-in, a major part of which is moving the system to a cloud-hosting provider.

The foundation for much of this transition work was laid in 2019 and 2020, when:

- Crossroads source code build processes were formalized and automated in Azure DevOps.
- Both vendor and state environment deployment processes were completely automated using Octopus Deploy.
- The release cadence for the Crossroads system was increased so new features and bug fixes could be released to users promptly.

In the years since, our automated deployment processes have enabled accurate and efficient system release updates with much less effort and without manual effort, a more reliable and stable approach. Additionally, in 2024, Voyatek implemented automated environment deployments for North Carolina's CACFP system, which we currently host for the state in the Microsoft Azure cloud. North Carolina's interest in moving the Crossroads system to the cloud dovetails well with our approach for automating build and deployment processes for both software and hosting environments.

The cloud offers many opportunities to improve hosting experience. Voyatek is focused on the following aspects:

- Increasing system reliability by leveraging the reliability features available in a cloud hosting environment, such as redundancy in compute, network, and storage
- Migrating to current platforms for server software and database
- Making system administration more secure by integrating with cloud user/directory management tools and ensuring administrative user identity using multi-factor authentication
- Simplifying the system architecture to address points of potential failure

Hosting Environment

The proposed Azure hosting environment will provide North Carolina WIC with several advantages. The primary hosting environment will be located in the East region. A region is a group of data centers managed as a single unit in Azure and known as "availability zones". Each availability zone is geographically separate and has redundant power and networking. The hosting environment will use a multi-zone configuration, which means that key elements of the infrastructure, such as the database, application servers, and storage, will run simultaneously in multiple physical locations. The system will continue to operate if an outage takes down infrastructure in a single availability zone. An incident that took down infrastructure in one availability zone happened in the CACFP system hosting environment in late 2024, and the system continued to work without noticeable impacts to users or system functions. Restoration of system functions likewise happened seamlessly without any interruptions or downtime. Bringing similar reliability to the Crossroads system will enable participants to continue to receive the benefits and services they are entitled to even if service outages occur in the hosting environment.

Some components of the hosting environment, including SQL Server and file storage, will be transitioned to platform-as-a-service (PaaS) services. These services are highly redundant, operating in at least three availability zones, with immediate and transparent failover

capabilities. These changes will improve the reliability and performance of the production Crossroads environment.

As an added protection, Voyatek will secure service reservations in a secondary region that is geographically distant from the US east region. These reservations provide a resource commitment that the compute capacity will be available in the event of an extended and broad outage in the east region. This will provide a secondary disaster recovery option to failover to a new region in the event of a large-scale regional outage.

Hosting Transition

The transition plan will utilize progressive tests of the transfer and system enablement process to verify production cutover readiness. The User Acceptance Test environment will be migrated using the production cutover plan to verify the process to:

- Transfer production data
- Transition NCID integration
- Transition CNDS and other services
- Redirection of URLs
- Migration of CDP EBT integration

Following successful migration of the UAT environment, the production transition will be scheduled and will utilize the procedures verified in the UAT migration. Voyatek anticipates being able to complete the production migration during a weekend with little or no impact to clinic operations.

Voyatek has successfully migrated the Rhode Island Crossroads hosting to our Azure Cloud. Voyatek is using a common deployment and hosting architecture for all Crossroads states including Rhode Island, Washington, and North Carolina. This does not mean that states will share infrastructure, but using a common approach will improve reliability and service delivery for all supported states. North Carolina's transition will utilize the successful transition model used by other Crossroads states which will reduce risk and minimize transition time.

WIC Crossroads Maintenance

b) Describe how Vendor will perform all maintenance to the WIC Crossroads application. Maintenance includes the following items:

- 1. Defect correction*
- 2. Change order implementation*
- 3. Production help desk support*

Voyatek's approach to maintenance and operations services delivery is based around a dedicated team of professionals with extensive knowledge of the North Carolina Crossroads systems. Voyatek has proposed a core team of staff including a product manager, business analyst, quality analyst, and software developer. These staff members are 100% dedicated to the North Carolina project except for the product manager who has a half-time allocation.

The assignment of a dedicated team improves productivity and the ability of the team to deliver high quality changes in a timely manner. During the release planning process, the product manager will work with North Carolina WIC staff to prioritize defect corrections and perfective changes to fully utilize the team's capability within the release cycle. While some larger changes that require additional staffing will utilize the change order process, smaller changes that can be prioritized for the core team can be worked without a change order process. During the current contract period, Voyatek has worked to deliver numerous perfective changes and to support Federal initiatives without having to utilize the change order process. Voyatek believes that a key differentiator of our services is to treat the core team as being dedicated to the WIC program and to allow them to be utilized to meet emerging needs with fewer change orders and unexpected costs.

Every member of Voyatek's proposed team has between 3 and 13 years of experience working with the Crossroads system and North Carolina's code base. This experience allows for faster resolution of defects and a higher volume of work produced. During the current contract period, Voyatek has worked to greatly reduce the defect backlog and to make significant improvements to the North Carolina Crossroad system.

Change Order Implementation

For larger changes that require the development of a change order, Voyatek staff work with North Carolina WIC to define needs and to develop a detailed change order proposal. Cindy Kochersperger, the project business analyst, has over ten years of Crossroads system experience and leads requirements gathering and creates the change order documentation. Our Crossroads experience allows team members to be more active participants in the change definition and design process which reduces demand on North Carolina WIC staff. Experience also reduces the likelihood of missed requirements and unexpected issues during the change process.

The Voyatek Nutrition practice maintains a large pool of experience WIC software development, mobile development, quality assurance, and business analysis staff. When change orders are needed, Voyatek can add knowledgeable staff to the change effort which further improves our ability to deliver high quality solutions. Voyatek has provided several significant change orders during the current contract period ranging from modern participant portal development to the improvement of Crossroads reports.

Help Desk

While this RFP describes what may be considered a more traditional help desk service, Voyatek has found that the day-to-day needs of the WIC program are best served by access to several key staff with extensive NC Crossroads knowledge and strong SQL query skills to investigate reported issues. As the current level 3 help desk, our experience has been that most North Carolina WIC inquiries are related to technical concerns that require skilled analysis. The project management, business analysis, and quality assurance team members provide this support and work directly with North Carolina WIC staff daily. Our goal is to make knowledgeable staff highly available to the WIC program and to provide timely support.

Voyatek maintains a traditional Help Desk staff, which can be contacted if project team members cannot be reached. This provides a secondary channel to allow NC WIC staff to reach a help desk during core hours of operation. The help desk will record the reported issue and contact team members for immediate response. Voyatek provides North Carolina WIC with direct contact information for all key staff, and since 2019, NC has not had to use our Help Desk. Voyatek understands the need to support programs during off hours to address issues prior to the start of operational hours.

A good example of Voyatek's commitment to support is our efforts to restore hosting operations following an extended outage due to technical concerns at the state data center. Voyatek staff were contacted at approximately 8 am on Saturday morning. The entire team was assembled and worked with North Carolina staff through midnight on Saturday and the following Sunday to restore program operations. The WIC system was the second public health system brought back online and benefits were remotely issued to 14,000 participants in time to prevent any gaps in benefit availability. Voyatek staff take pride in their ability to work with WIC programs to deliver services to participants.

WIC Crossroads Enhancements

c) Describe how Vendor will perform enhancements to the WIC Crossroads application in accordance with the Change Request process Section 3.5 Business and Technical Specifications, Sub-Section 3.5.11.

Voyatek's project management and quality assurance staff have extensive experience working with North Carolina WIC's change management process. The teams experience with Crossroads and North Carolina WIC policy improves the ability to design effective solutions and to be knowledgeable participants in the enhancement process. Voyatek also works to bring innovative solutions developed for other WIC programs to streamline and improve the efficiency of Crossroads enhancements.

During the current contract period, the North Carolina WIC program has been faced with a series of challenges ranging from weather events, Covid related waivers, formula shortages, and other short notice Federal policy changes. Voyatek has adapted with North Carolina to rapidly respond

to enhancement and change needs. Voyatek has also worked successfully with North Carolina to implement several major Crossroads changes with little or no disruption to the program. These have ranged from the improvements to the Not-to-Exceed calculation processes to the deployment of the participant tele-health portal.

Voyatek believes a key service differentiator is our ability to bring in specialized skilled staff to assist with activities like web portal design, responsive web portal development, EBT enhancements, and upgrades based on the transfer of existing solutions within other WIC systems.

Transition-Out Services

d) Describe how Vendor will provide “Transition-out” services. (A description of a detailed Transition-Out plan is requested in Section 3.5 Business and Technical Specifications, Sub-Section 3.5.14.)

Voyatek recognizes the importance of providing consistent services and supporting the orderly transition at the end of a contract period. We know that this could be the transition to a new M&O vendor or to support the migration to a new WIC MIS platform. Voyatek has provided a Transition-Out Services plan as [Appendix L](#). Voyatek will maintain knowledgeable staff through the transition period to support a smooth transition.

Voyatek understands that these services include maintaining a knowledgeable and capable staff to support the project through project completion. Project staff will support the transition of project documentation, transfer of issue management data, transition of software source code data, and the transfer of North Carolina WIC data managed on behalf of the State. Project data will be disposed of as per North Carolina data handling policies and procedures.

WIC EBT Consulting and Training

e) Describe how Vendor proposes to conduct all necessary Crossroads related consultation and training of the WIC EBT Provider and EBT FMNP staff at no additional cost to the State. (A description of Vendor’s specific training approach is requested in Section 3.5 Business and Technical Specifications, Sub-Section 3.5.4 and 3.5.5).

Voyatek leads the industry in EBT Universal Interface support in WIC MIS systems. Voyatek was the first vendor to adopt the current JSON-based standards found in the 2022 WUMEI specifications. And Voyatek is currently building the first MIS framework to support the full transaction set of the 2022 WUMEI and, coincidentally, is testing the new framework with North Carolina’s current EBT provider. When North Carolina decides to transition to the 2022 WUMEI, the Voyatek team will work with the State’s EBT provider to efficiently transition to the new interface. As part of that transition, we will provide consultation, collaboration, and training as needed for the EBT provider and FMNP staff at no additional cost to the State.

3.5.3 Product Management

a) Product Staffing

Describe your staffing plan for this contract. (After contract execution, pursuant to the DIT Terms and Conditions, the Vendor will request prior written State approval for changes to personnel who fill the role of any of the Personnel described in this RFP prior to personnel changes occurring. The State also reserves the right to reject any replacement and reserves the right to request a replacement should the State deem it necessary.)

Voyatek Nutrition Practice

Before describing the details of our proposed team, it is important to understand the extensive and experienced organization that supports our proposed NC support team.

Voyatek has been managing WIC systems for over two decades and supports a wide range of WIC programs across the country on two WIC MIS platforms: WoW, short for WIC On the Web and Crossroads, the latest and largest of the state agency model (SAM) systems sponsored by FNS for which North Carolina led the development of. WoW and Crossroads contain the greatest functional profiles of WIC MIS systems in use today and together support over half of the WIC participants in the country. This diversity of experience and functionality enables Voyatek to share ideas and experiences between state programs to the benefit of our customers.

An additional benefit of our large customer base is our ability to assign focused support teams to each project while, at the same time, maintaining sufficient resources to cross-train other team members or new hires so we can respond to the needs of our customers quickly and efficiently.

The organization chart in [Figure 1](#) below depicts the reporting structure within Voyatek's Nutrition Practice, which is led by Krushanu Majmundar, who is responsible for service delivery to our current clients, and Jay Saunders who is responsible for nutrition product development. Krushanu and Jay report to Rich Corey, who leads our Health & Human Services business. Rich reports to Lisa Mascolo, Voyatek's Chief Executive Officer (CEO).

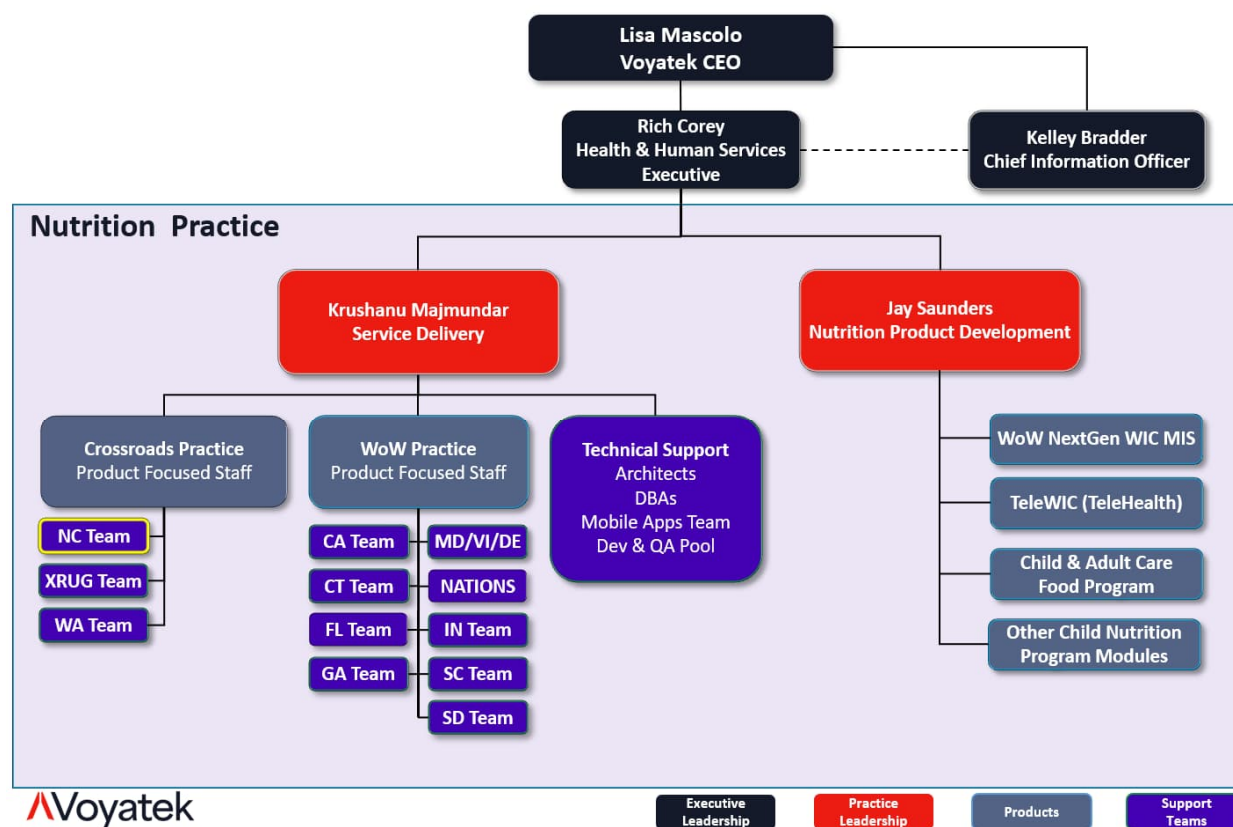


Figure 1: Voyatek's Nutrition Practice Organization Chart

Kelley Bradder, our CIO, manages the IT Support Services organization within Voyatek that provides and manages hosting platforms and security solutions. Kelley work closely with Krushanu and Jay to support Voyatek's Nutrition Practice's needs from their organizations.

Nutrition Practice Organization Design

Over the past five years, the technological landscape has undergone a substantial shift, transforming the way software is designed and delivered. Rahul Puri, Voyatek's Chief Strategy Officer, recognized the need to prioritize technological innovation in the federal nutrition space, particularly because most MIS systems administering programs in this domain rely on legacy technology. Rahul played a crucial role in establishing the Nutrition Product Development division, which is dedicated to driving technological innovation and developing new products and services. Jay Saunders was chosen to lead this division due to his extensive prior product focused experience in the WIC and public health domains, which includes his prior leadership of the development of the Crossroads WIC MIS. Jay's organization focuses on designing and prototyping new products for the future, the next generation of technology. Their work includes the cloud native next generation MIS system architecture for reduced costs with maximum dependability and an innovative telehealth solution to support the new ways in which healthcare is delivered.

In addition, Jay leads the development of new solutions for the child nutrition program (CNP), starting with the Child and Adult Care Food Program (CACFP) as the first module in the system.

Krushanu's organization includes the Crossroads Practice and the WoW Practice, each dedicated to excellence in their support of their respective system products. Krushanu's focus is on meeting the needs of Voyatek's clients every day to enable them to provide for the citizens they serve. [Voyatek is particularly proud of the accomplishments of our Crossroads Practice, which now includes supporting all states running the Crossroads WIC MIS nationally.](#) In January 2025, Washington State selected Voyatek to assume M&E support for their version of Crossroads, further enriching the depth of our Crossroads experience and enabling the sharing of even more ideas between Crossroads states.

By maintaining separate teams focused on the demands of today and the needs of the future, Voyatek avoids the challenges faced by many organizations where today's problems usurp the time and energy needed to invest in the future. This dual focus on current clients and new products enables Voyatek to maintain exceptional support for our current customers while fostering a collaborative environment where the delivery team can share its valuable experiences and insights with the product team. This cross-functional exchange of knowledge facilitates the creation of technologically advanced products that are not only innovative but also firmly grounded in practical business functionality to address the unique challenges and opportunities within the federal nutrition space and especially the WIC program. By integrating cutting-edge technology with sound business principles, Voyatek delivers nutrition solutions that enhance efficiency, effectiveness, and user satisfaction for our customers.

While we do not anticipate a change in staffing from our proposed personnel, Voyatek understands that unforeseen circumstances may require resource shifts. Our WIC Practice includes 80+ professionals with deep WIC experience that will be drawn upon to support the NC project in the event staff changes are required. In these circumstances, our proposed product manager, Jennifer Saunders, will work with Krushanu Majmundar to identify a staff member with comparable skills and availability. Jennifer will present North Carolina with the person's resume for State approval prior to replacing the staff member. Voyatek understands that the State reserves the right to reject any replacement candidate. We also understand that the State reserves the right to request the replacement of an existing team member should the State deem it necessary.

[Voyatek NC Crossroads Support Team](#)

Voyatek is proposing the same highly qualified team that supports North Carolina today. Our team brings a depth of Crossroads experience and specific knowledge of North Carolina's version of Crossroads as well as NC processes and standards that enable them to provide an outstanding level of support for the State. The following sections of our proposal detail the four positions that

we consider key to the success of the project and the highly qualified people that Voyatek is proposing for those key positions:

- M&E Vendor Product Manager – Jennifer Saunders
- M&E Vendor Development Manager – Michael Heinrich
- M&E Vendor Test Manager – Helena Young
- M&E Vendor Business Analyst Manager – Cindy Kochersperger

Resumes for key personnel are included for reference in [Appendix S: Key Personnel Resumes](#).

M&E Vendor Product Manager – Jennifer Saunders

The State envisions a product team that includes the following Personnel, or Vendor's equivalent position/title in 1-4 below:

1. M&E Vendor Product Manager – Describe how this position leads the Vendor's team and is responsible for the overall management of the Contract and the completion of all required tasks and activities during the Contract. Please include the name and describe the relevant experience and qualifications of the proposed person. In lieu of the description, Vendor may provide a Curriculum Vitae (CV) for the resource proposed for this position.

Voyatek proposes to have Jennifer Saunders continue in the role of M&E Vendor Product Manager. Jennifer is a seasoned project manager and PMP (Project Management Professional) with over 25 years' experience providing services in the government sector, specializing in social services. For the last 15 years she has been successfully delivering, managing, and coordinating WIC software implementation and support projects. Her strengths are account management, risk analysis and mitigation strategies, budget and schedule management, planning, and project execution. [Jennifer has led M&E work on three different WIC MIS systems and currently leads our North Carolina Crossroads M&E support team](#), working closely with North Carolina to collaborate and coordinate the work.

The Voyatek product manager is responsible for overall project execution and completion of project deliverables. Jennifer will manage the daily work of the Voyatek team and coordinate contract work with North Carolina WIC. Her responsibilities include:

- Serve as the primary point of contact for the contract and project for North Carolina WIC and other NC entities
- Provide both contract administration and project management throughout the contract
- Coordinate Voyatek resources for execution of the WIC MIS project with full authority to commit Voyatek on matters concerning the contract
- Timely development of project deliverables and services, within scope and within budget
- Develop project plans and objectives, involving all relevant stakeholders and ensuring technical feasibility
- Oversee resource availability and allocation

- Develop a detailed project plan to track progress
- Use appropriate verification techniques to manage changes in project scope, schedule and costs
- Measure project performance using appropriate systems, tools and techniques
- Report and escalate to management as needed
- Manage the relationship with North Carolina WIC and stakeholders
- Perform risk management to minimize project risks
- Establish and maintain relationships with third parties/vendors when needed
- Create and maintain project management documentation
- Notify the Crossroads WIC MIS Release Manager, verbally within one business hour and in writing within one business day, when Voyatek discovers any problem(s) that may jeopardize the successful or timely completion of our contract obligations.

M&E Vendor Development Manager – Michael Heinrich

2. M&E Vendor Development Manager – Describe how this position leads the Vendor's technical team during both the Transition-In Phase and M&E Phase (including transition-out) of the Contract and assists the State in ongoing technical management. Please include the name and describe the relevant experience and qualifications of the proposed person. In lieu of the description, Vendor may provide a Curriculum Vitae (CV) for the resource proposed for this position.

Describe the responsibilities of this position for:

- a. Generating System designs;*
- b. Coordination and execution of the system interface between Crossroads and the EBT system;*
- c. Coordination and execution of the Crossroads system configuration and architecture changes.*

Voyatek proposes to have Michael Heinrich continue in the role of M&E Vendor Development Manager. Michael is a software engineer with 20 years of demonstrated experience in the software development industry. He is a strong “full stack” (all aspects of platform development) business software development professional skilled in C#/.NET, EF, HTML, CSS, MS SQL, Oracle, Bootstrap, jQuery, LINQ, WordPress, MySQL, and Python.

The Voyatek Development Manager will provide leadership for the technical team throughout the contract, including the important Transition-In work to rehost the NC Crossroads system to the Azure cloud. Michael's responsibilities include:

- Manage the software build baseline, including management of system configuration and architecture changes
- Provide daily technical guidance for the development team
- Develop necessary user interface software to meet requirements, including maintaining and enhancing the critical interface to the EBT system.
- Develop necessary system interface software to meet requirements
- Develop necessary software/scripts to manage database layer

- Develop necessary software to manage business operations layer
- Lead the optimal application of technology and engineering resources to meet customer requirements
- Maintain and support the system design for approved enhancements

M&E Vendor Test Manager – Helena Young

3. M&E Vendor Test Manager – Describe how this position leads the Vendor’s testing team during the Contract. Please include the name and describe the relevant experience and qualifications of the proposed person. In lieu of the description, Vendor may provide a Curriculum Vitae (CV) for the resource proposed for this position. Describe the responsibilities of this position for:

- a. Functional, End-to-End, System life cycle, and performance testing oversight during maintenance and enhancement phases;
- b. UAT testing oversight and support;
- c. Test script or other artifact development;
- d. Test reports

Voyatek proposes to have Helena Young continue in the role of M&E Vendor Test Manager. Helena is a senior Quality Assurance professional with over 20 years of experience in testing software solutions and migrating data into new solutions, **including 14 years of experience on the Crossroads system and as the original QA lead for the development of the system.** She has worked extensively in system testing, user acceptance testing (UAT), functionality testing, black box testing, integration testing, and regression testing. Helena is an expert in data conversion, application testing, and back-end testing. She will manage all testing efforts, including end-to-end system testing, regression testing, and performance testing.

The Voyatek Test Manager will provide leadership for the testing team throughout the contract. Helena’s responsibilities include:

- Manage the overall end-to-end system testing processes during maintenance and enhancement phases inclusive of User Acceptance Testing (UAT)
- Maintain and manage well-established test processes in a team environment
- Test highly complex code and integrated system capabilities
- Confirm that the system functions correctly across different environments
- Conduct tests to verify user functionality and system configuration
- Investigate and resolve matters of significance for end-user problems
- Write test scripts, test reports, requirement documents and other related technical documents
- Produce test reports to summarize testing activities for clients

M&E Vendor Business Analyst Manager – Cindy Kochersperger

4. M&E Vendor Business Analyst Manager – Describe how this position leads the Vendor's Business Analyst team during the Contract. Please include the name and describe the relevant experience and qualifications of the proposed person. In lieu of the description, Vendor may provide a Curriculum Vitae (CV) for the resource proposed for this position.

Describe the responsibilities of this position for:

- a. Creating Change Requests Responses and Estimates;*
- b. Supporting Help Desk assistance requests, including data correction;*
- c. Ensuring test scripts and other artifacts to satisfy State business needs*

Voyatek proposes to have Cindy Kochersperger continue in the role of M&E Vendor Business Analyst Manager. Cindy is a business analyst professional with over 30 years of experience in the Information Technology industry. She began her IT career as a developer, which provides her with a technical background, a valuable perspective for business analysis work. Cindy consistently delivers quality projects on time with high customer satisfaction. Her excellent interpersonal and communication skills enhance both client and internal relationships. **Cindy has over 12 years of developing and supporting systems for the WIC program across five states, including 10 years of support and leadership on the Crossroads system.**

The Voyatek Business Analyst Manager will lead business analysis activity throughout the contract. Cindy's responsibilities include:

- Manage the overall requirements and requirements verification process
- Lead and create change requests responses and estimates
- Provide daily technical guidance for the business analysts
- Work with well-established processes in a team environment
- Validate that workflow in the system is optimized
- Confirm that customer requirements are accurately reflected in the system and in system documentation
- Validate that test scripts satisfy North Carolina's business requirements and needs
- Support the North Carolina Help Desk, including assisting with data corrections

M&E Vendor Advisory Technical Architect – Jon Moreau

Voyatek is proposing Jon Moreau as an Advisory Technical Architect to support Michael Heinrich and the technical team for system architectural guidance when needed. While the system's architecture is stable and proven, the transition to the cloud offers potential opportunities to make architectural adjustments that leverage cloud capabilities. Jon has over 20 years of system technology engineering experience, with 10 years of WIC and CACFP (Child & Adult Care Food Program) experience on various systems. He focuses his time and energy on designing and building architecture for next-generation government systems. Jon just completed designing Voyatek's next generation architecture for our CACFP state system now running in North

Carolina, NC Connects. In the process, he conceived what is becoming our next WIC MIS framework. Prior to that, Jon was the technical architect for the Crossroads WIC SAM system. Jon's career focus is on engineering technical solutions to complex problems.

The Advisory Technical Architect will be responsible for the technical architecture and guiding the evolution of the Crossroads system as it transitions to the Azure cloud platform. Jon's responsibilities include:

- Directing the optimal application of technology and engineering to meet North Carolina requirements
- Leading system changes to take advantage of cloud platform capabilities
- Supporting the team as needed with system architecture questions and guidance

5. Describe and diagram the organization of the proposed product team, including identification of the key Personnel noted above by name, position title, and responsibilities, lines of authority among and between the various Personnel and any subcontractors that may be used on this product, and whether any Personnel will be hired upon Contract award. Include available letter(s) of intent to accept employment from any such Personnel that are to be hired after Contract award.

The organization chart in [Figure 2](#) below depicts the Voyatek support team and executive support in relation to the North Carolina WIC organization. Key personnel are depicted with a small black key symbol in the upper right corner of their organization box. No subcontractors are shown because Voyatek will not be engaging subcontractors to provide support for NC Crossroads.

Because this is the same team supporting North Carolina WIC today, no additional hires are currently planned. All proposed personnel are Voyatek full-time employees. Upon the Contract award, the team will be available to plan and support the rehosting of NC Crossroads to the Azure cloud while continuing the steady and dependable M&E support that North Carolina requires.

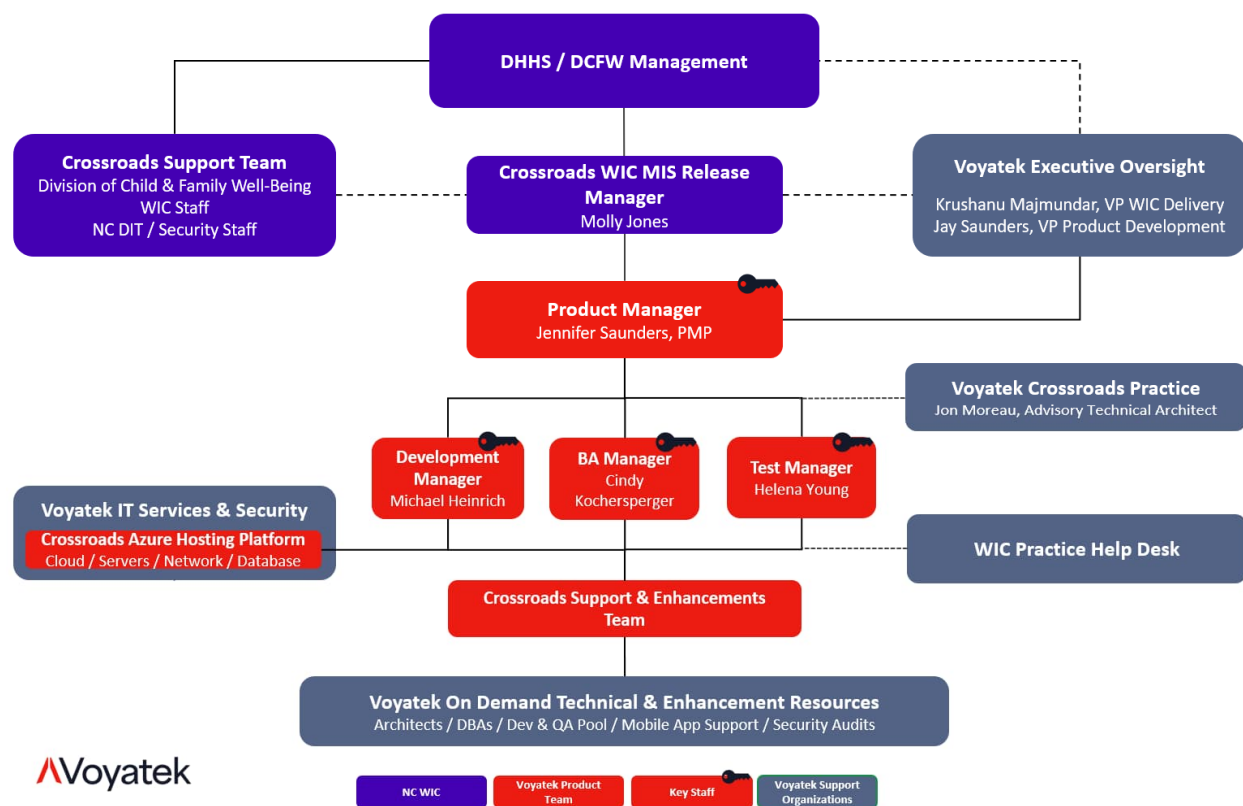


Figure 2: Voyatek's WIC Cascades Product Team Organization Chart

In addition to the core NC product support team described above and shown in red on the organization chart, the chart also reflects the depth of additional support from the greater Voyatek organization:

- ✓ **Executive Oversight:** Krushanu Majmundar and Jay Saunders will provide executive oversight and a point of escalation for any project issues requiring higher level Voyatek input.
- ✓ **Information Technology Services & Security (ITSS):** This group reports to Kelley Bradder, Voyatek's Chief Information Officer (CIO), and provides the Nutrition Azure Cloud, our proposed new hosting platform for NC Crossroads. The ITSS team is an experienced full-service hosting organization that provides platform support and hosting for Voyatek systems as well as client systems both on premises and in several clouds.
- ✓ **Crossroads Practice:** This is a Voyatek organization supporting the Crossroads User Group and Washington State in addition to North Carolina. The practice shares ideas and information across dedicated teams and provides technological leadership such as Jon Moreau architectural insights. Jon was the original architect that helped to design Crossroads.

- ✓ WIC Practice Help Desk: Our Help Desk spans multiple accounts in our WIC Practice. It will provide backup support for the NC product support team should they not be available when needed.
- ✓ On-Demand Technical and Enhancement Resources: This pool of resources provides extensibility for the NC core support team. These resources are shared as needed across our Nutrition and WIC Practice to provide expertise in specific technical areas such as database administration, mobile app development, security, etc.

6. Describe how Vendor will ensure that the Personnel resources are readily available to the State and how those resources will be able to fully support the Crossroads product.

As noted above, the team that Voyatek is proposing for support of NC Crossroads in the next contract is the same team that North Carolina depends on today. Voyatek commits to providing these key resources to continue providing excellent support for the State in the next contract.

7. Describe how the State will be able to contact Vendor Position resources, and the escalation path that would be followed to ensure that the State can establish contact with the personnel who fill the role of any of the Personnel when critical needs arise and during critical product periods between the hours of 7:00 am and 7:00 pm Eastern Time, seven (7) Calendar days a week.

Voyatek understands that information technology system support sometimes requires immediate action by technical team members at any time of the day. We endeavor to provide stability and dependability in our solutions to avoid these types of circumstances but acknowledge that unanticipated events can sometimes disrupt the best plans and system design. To provide optimal support, we provide direct access contact information for the lead product team members so that North Carolina can contact the team directly when needed. We do not constrain our customers to work through a personnel hierarchy to get to the key staff when a critical need arises. This level of support provides flexibility and speed of response outside of normal business hours that the State can depend on, as the Voyatek team has demonstrated whenever needed as part of our support in the current contract.

Contact information, including mobile numbers, will be provided for all core support team members. North Carolina will also have access to contact information for management staff that act as a point of escalation should need arise. Krushanu Majmundar, the Senior Vice President, is the primary point of escalation, and Rich Corey, the HHS Industry Lead and a member of the Executive Leadership Team, provides a second point of escalation. Jay Saunders provides Crossroads experience and technical guidance to the team. He is available, as needed, to assist with issues as they arise. Voyatek will also provide a help desk number that can be used in the event that no team member can be reached. The help desk operates during the North Carolina critical periods of operation and can record issues reported to it. The help desk will coordinate

their responses with a Crossroads team member. The Voyatek Crossroads team has worked to be highly available and responsive to North Carolina WIC needs at any time of the day.

8. Describe the staffing approach to include any subcontractor staff.

Voyatek does not plan to use subcontractors in support of the NC Crossroads WIC MIS. Our team and depth of talent in our WIC Practice will provide all M&E support responsibilities and our IT Support Services division will provide all support for Azure cloud hosting.

9. Describe specific steps the Vendor will take to ensure retention of applicable staff during transition-out, to remain compliant with all Contract requirements and SLA until the Contract expires or is terminated.

As described above in [c\) Transition-Out Period](#), Voyatek understands that the most important element in the transition of support for any system is the coordination and collaboration between the incoming and outgoing contractors. In the event we are not chosen as the subsequent M&E service provider, we will support a smooth transition to a new M&E provider, including retention of our staff to properly transition knowledge, system code, documentation, and artifacts to the next vendor. Due to the size of our WIC and Crossroads teams, Voyatek will seek opportunities for reassignment for team members following contract conclusion. This makes early departures by qualified staff less likely and allows Voyatek to continue to fully staff the project throughout the contract period.

10. The following are the current roles and responsibilities for the North Carolina DHHS WIC solution, for the Vendor to consider in its proposed organization. Figure 2 illustrates the Organization Structure. (NC DHHS WIC org chart and responsibilities from the RFP not included for brevity.)

Voyatek has reviewed and understands the North Carolina DHHS WIC team structure. In our proposed organization chart above, we have included our understanding of the North Carolina organization and how our team will interact with NC WIC. We look forward to continuing our working relationship with the NC team.

b) Product Management Plan

Describe Vendor's Product Management Plan (PMP) that outlines Vendor's proposed product management approach for this product. The Product Management Plan is the overarching "umbrella" Plan that defines how the contract is executed, monitored, controlled, and closed. Vendor may provide the plan description within the body of the text of the Vendor's proposal or provide a separate section or attachment.

Voyatek's draft Product Management Plan has been provided in [Appendix B: Product Management Plan](#).

Describe the following:

1. The points of contact between the Vendor and the State and the level of decision-making authority these positions will have.

The primary points of contact between the State and Voyatek for the day-to-day performance of the contract will be the interactions between the DHHS Crossroads WIC MIS Release Manager and Voyatek's Product Manager, Jennifer Saunders. As the current M&E Vendor Product Manager supporting North Carolina, Jennifer is in regular contact with the Crossroads WIC MIS Release Manager throughout each week, updating the State on our progress and alerting the State to concerns or challenges as our work proceeds. We use our weekly status calls with the State to provide a regular cadence for formal discussion of contract progress but also have utilized regular unscheduled communications to allow the State to be aware of our progress and, if potential obstacles or risks are encountered, the State is made aware of them as well as alternatives for mitigating those obstacles or risks in real time.

Jennifer Saunders has full decision-making authority within the contractual obligations of the Voyatek support team. Krushanu Majmundar has full authority for additional resources needed to support the contract, for contract amendments, or any other Voyatek commitment requested or desired by NC WIC.

As shown in our proposed team organization chart above, we provide an escalation path above Jennifer Saunders to Krushanu Majmundar. Krushanu is a Senior Vice President, one level below the ELT and leads our Nutrition Delivery Practice to serve as the executive point of contact for support, guidance, and accountability within Voyatek. Jennifer reports to Krushanu and keeps him informed of our contract progress, accomplishments, plans, and challenges. Krushanu is available to the Crossroads WIC MIS Release Manager and/or the DHHS management team at any time.

2. The proposed levels of staffing, including technical staff, to ensure all deployment, ongoing, and transition-out operational tasks and responsibilities are completed in a timely and accurate manner. At a minimum, Vendor's proposed levels of staffing will be such that the following specifications can be met:

- a. Notifying designated State staff within one (1) hour in the event a situation occurs that might adversely affect system deployment, ongoing system operations, or 3rd party system such as EBT.*
- b. Providing a Change Request (CR) Response as outlined in the Change Request Process.*
- c. Providing CR Draft Estimates as outlined in the Change Request Process.*
- d. Providing appropriate technical staff so that approved CR Estimates are developed, tested, and delivered for UAT as outlined in Change Request Process.*
- e. Providing appropriate technical staff for the timely and accurate correction of all system defects in accordance with all SLA requirements. A temporary workaround for production down or critical system defects with the core business processes that prevent the certification of WIC participants, the issuance of WIC benefits, reconciliation of redeemed benefits, generation of rebates, and transmission/reception of EBT files will be developed and implemented as stipulated in Table 3 - Service Level Agreement.*

Voyatek's seasoned and experienced NC WIC support team are proposed in alignment with the services requested by the RFP. Our Development Manager (Michael Heinrich), Test Manager (Helena Young), and Business Analyst Manager (Cindy Kochersperger) are all full-time resources dedicated to the support for North Carolina. Our Product Manager (Jennifer Saunders) supports

North Carolina approximately half time as she splits her time with another project but is available to the State at any time during business hours. Supporting our team managers are other resources as needed based on the timing of the release work and the specific scope of each release.

This seasoned team is fully prepared to meet all North Carolina contractual requirements and commitments in support of the NC WIC team, including:

- ✓ Notifying designated State staff within one hour of a situation that might have an adverse impact on the NC Crossroads production systems.
- ✓ Carefully following the NC Change Request Process to provide timely and detailed change request estimates, including providing draft change request estimates and then collaborating with the NC WIC team to refine the draft estimates to arrive at final estimates.
- ✓ Providing qualified and experienced technical staff to deliver approved change requests to UAT on time, on budget, and with high quality.
- ✓ Providing qualified and experienced technical staff for the timely and accurate correction of all system defects in accordance with the contractual service level agreement included in as Table 3 in the RFP.

In addition, as we transition into the new contract, our Information Technology Services & Security (ITSS) team will be engaged to support our NC team as we rehost NC Crossroads to our Nutrition Azure cloud. ITSS provides a matrixed support team of cloud, server, database, network, and security specialists who will work with Michael Heinrich in establishing and providing the Azure hosting platform and support.

3. The industry best practice development methodology to be used by the Vendor, adhere to best practices for development coding standards, and include detailed comments within the source code, using only the English language, explaining system modifications and issues resolved.

Voyatek developers adhere to the software industry's best practices as well as specific coding standards for their respective system. All comments in the system code are done in English. For NC Crossroads, the Development Manager will perform peer reviews to verify the produced code meets quality standards and require developers to perform the following steps as they develop or modify the Crossroads source code:

1. Maintain development checklists.
2. Write meaningful comments to describe complicated business logic.
3. Provide check-in comments when code is committed to source control.
4. Link user stories and bugs to the checked-in change sets to enable backward tracking.
5. Perform unit testing.

The Voyatek Nutrition Practice utilizes Git for source code management, one of the software development industry's best practices and a Microsoft-recommended methodology. Git's distributed version control system allows developers to work on their copies of the source code independently, providing a flexible and efficient environment. With decentralization each developer has their repository, enabling them to make changes, experiment with new features, and address issues without affecting the main codebase. Git's branching and merging capabilities are instrumental in facilitating parallel development efforts. Developers can create branches to isolate their work and once the changes are complete and tested, Git enables the merging of these branches back into the main codebase. This approach not only empowers developers to work independently on diverse tasks but also facilitates a smooth integration of their contributions into the overall codebase, promoting collaboration and minimizing conflicts. The use of Git-based version control fosters a collaborative and agile development environment leading to heightened quality and efficiency throughout the software development lifecycle.

4. How Vendor will provide staffing for the Help Desk so that all incoming calls, emails, or issues in the reporting system are answered within the period defined in the SLA.

Voyatek provides direct contact information for our Crossroads product management team members so that NC WIC has the most efficient support for the State Office staff, including the State Help Desk. In addition, we maintain a central WIC help desk with operating hours that correspond to North Carolina's normal business hours and with a dedicated unlimited call, toll-free phone number to provide prompt support to NC WIC staff for reported issues. Our help desk team records reported issues in their issue management system and contacts our Crossroads support team to initiate a timely and efficient response. These two methods of reaching our Crossroads support team enable the NC WIC team to have their questions and issues addressed promptly. In addition to phone calls, for lower priority issues, the NC WIC staff may opt to send emails directly to our team. The Crossroads product team has a demonstrated track record of being responsive and efficient in tracking and resolving issues for NC WIC in a manner consistent with the requirements of the SLA.

5. The Vendor's product management approach to ensure that the above SLA requirements are met.

The key to meeting service level obligations is proper team staffing, training, and focusing on excellent customer support. Across our WIC Practice customer base, Voyatek has a track record of success with a variety of SLAs. The Voyatek product manager will monitor and measure the Voyatek team's performance against all North Carolina service level requirements in the SLA. Further details on our approach to SLA management can be found further down in this section in the subsection on "Service Level Agreement." We are proud to report that Voyatek has had no cited SLA issues during the current contract period. This reflects our commitment to delivering reliable, high-quality service while consistently meeting or exceeding performance expectations.

6. Vendor's experiences with meeting time-sensitive special needs of a state agency. For example, describe any experiences with implementing MIS functionality changes as part of a state's response to COVID-19.

Voyatek staff take pride in their ability to work with WIC programs to deliver services to participants. We foster a 'customer-first' culture among our staff, which is evident in the support provided to our customers. During the COVID-19 pandemic, project staff demonstrated their willingness to go above and beyond, exemplifying this culture. Swift response to state policy changes, such as the increase in Cash Value Benefits (CVB) for participants, was made possible through the collective efforts of our staff across our various WIC projects.

As mentioned previously, a good example of Voyatek's commitment to support is our efforts to restore North Carolina's hosting operations following an extended outage due to technical concerns at the state data center. Voyatek staff were contacted at approximately 8 am on Saturday morning. The entire team was assembled and worked with North Carolina staff through midnight on Saturday and the following Sunday to restore program operations. The WIC system was the second public health system brought back online and benefits were remotely issued to 14,000 participants in time to prevent any gaps in benefit availability.

Recently, when North Carolina transitioned the FMNP solution from paper to EBT, the Voyatek team collaborated with the State and the EBT provider to design an innovative solution for Crossroads that kept the FMNP data properly isolated in the Crossroads system and to provide a new interface to the Farm Market system on a schedule that allowed the State to get the FMNP benefits out to participants in time for the growing season. Throughout the project, Voyatek was flexible in our design in response to requirements from the EBT provider, providing the ability to meet the project deadline.

7. Other aspects, if any, of Vendor's proposed product management approach.

Voyatek is an active partner in addressing evolving FNS policies and WIC program needs. One advantage of working with Voyatek is our ability to respond to changing FNS policies and evolving challenges to the WIC community. For example, when new policy updates are published, we create a cross-team work group consisting of team subject matter experts with state agency experience, technical and project leaders to review policy guidance and design proposed solutions that meet new policy requirements. We include alternative solutions to meet WIC program expectations and identify program differences to share with state WIC staff. The goal is to develop reusable and transferable updates and procedures that allow states to efficiently implement changes. This approach has allowed Voyatek states to respond promptly to recent changes with Cash Value Benefits policy, Covid related waivers, not-to-exceed (NTE) calculation efficiencies, and formula shortages. As similar opportunities arise in the next contract, the Voyatek project team will be prepared to provide proactive analysis and options to NC WIC based on North Carolina program requirements.

Most Voyatek states maintain independent code bases for their WIC MIS. Voyatek has worked to develop transferrable enhancements to allow for the sharing of improvements while maintaining each state's MIS independence. We have used this approach in the development of participant portals, mobile applications, help desk modules, breastfeeding peer counseling modules, and EBT WUMEI support. As an example, the Help Desk Module was first developed for WoW states and then adapted for use in Crossroads. The module allows state help desk staff to address several common support issues that previously required M&E vendor support such as changing a participant's gender or date of birth. The module creates an audited interface that performs updates and automatically checks for potential impacts like changing a participant's certification status because of an age change. The Help Desk module improves the speed and reliability of common help desk corrections and allows for more effective use of staff time.

Voyatek is leveraging our experience building transferrable solutions as part of the transition to modern software and hosting frameworks while building next generation WIC solutions that integrate with both WoW and Crossroads systems. The first phase of this process is in progress and will modernize EBT, rebate, NTE, benefit redemption, and food management systems. The next phase, planned to commence in the second quarter of 2025, will transition vendor management and add new analytics capabilities.

c) Transition-In Phase Plan

The purpose of the Transition-In Phase is to facilitate the transition of full responsibility for supporting Crossroads from the incumbent vendor to cloud environments managed by the awarded Vendor.

1. Describe Vendor's proposed Transition-In Plan to address how Vendor will perform the tasks needed to successfully transition Maintenance and Enhancement Services from the previous Vendor.

2. Describe in your Transition-In Plan in detail, Vendor's approach to each of the following Transition-In Phase specifications:

- a. Coordinate an onsite Kickoff Meeting within four (4) weeks of the Contract effective start date, with appropriate State staff and the incumbent Crossroads vendor, to be held at State facilities in Raleigh, North Carolina.*
- b. Attend any additional training sessions with the incumbent vendor, either virtual or onsite, as requested by the State, at a location within or outside of North Carolina, to be determined by the State.*
- c. Transition-in the Crossroads source code and system documentation from the incumbent vendor, to compile and produce the Vendor's first installable internal system test build of Crossroads within ninety (90) Calendar Days of Contract Execution.*
- D. Request any needed State-owned hardware for consideration by the State for approval.*
- e. Submit applicable Document Deliverables listed in Table 1 – List of Product Deliverables*
- f. Import DFDD and Risk Code documentation, User Manuals, DTS and White Papers, Data Dictionary, ICD, ECD, RDD, Installation and Configuration Instructions, and the CPS Operations Manual.*
- g. Import regression and performance test artifacts.*
- h. Begin Change Request and Release planning and execution for M&E Phase.*
- i. Deploy issue reporting system and secure FTP site.*
- j. Deploy action item tracking tool.*
- k. Deploy collaboration web site.*

l. Deploy Help Desk contact infrastructure.

m. Request all needed access and NCID credentials for State environment support.

n. Obtain and submit signed Non-Disclosure Agreements within fifteen (15) Calendar days of Contract Award for all Vendor staff who will have access to Crossroads Confidential Information.

o. Deploy the Vendor's internal development and test environments needed to compile and install changes to the source code.

p. Deploy functioning solutions of the WIC Crossroads solutions (applications and data including file systems) into the Vendor managed cloud environments for State production, State UAT, and State Staging within one hundred twenty (120) Calendar Days of Contract Execution. Any changes to the Crossroads systems needed to successfully integrate them into the cloud platform will be performed at no additional cost.

q. Provide State personnel (to be determined at the sole discretion of the State) with all necessary access credentials, database permissions, training, and client software requirements needed to execute read-only (R/O) queries and other scripting against all production and non-production Vendor-managed databases

r. At no additional cost, the Vendor will obtain all necessary third party software/ IaaS/ PaaS/ SaaS licenses for Vendor's Services for the Crossroads solution in the Vendor-managed Production and non-Prod environments, including but not limited to cloud computing platforms, networking services, operating systems, database software, software deployment solutions, and storage.

Voyatek's draft Transition-In Plan addresses these requirements and has been included in our proposal as [Appendix A: Transition-In Plan](#).

d) Joint Application Design (JAD) Sessions for Change Requests

Describe the approach and types of JAD sessions the Vendor would facilitate to develop specific requirements to implement Change Requests. The Vendor will have designated staff, that is not facilitating the meeting, present and available to document decisions and action items. All JAD sessions will be conducted either virtual or in Raleigh, North Carolina, to be determined by the State. Onsite sessions in Raleigh may be required only for significant new functionality.

For change request work, Voyatek will collaborate with NC WIC through our Joint Analysis & Design (JAD) sessions. JAD sessions will be either in-person meetings in Raleigh or virtual interactive meetings depending on the depth and complexity of the change request under consideration. During the JAD session, the system feature design will be discussed with NC WIC, weighing the pros and cons of various solutions. To efficiently run these meetings, Voyatek provides multiple staff to participate:

- **Facilitator** – This person's focus is keeping the meeting moving, drawing out participants, and focusing on the meeting objective.
- **Scribe** – This person records the meeting decisions and key elements of the discussion that will contribute to a good final design.
- **Subject Matter Expert(s)** – Voyatek staff who know the system's current functionality best for the system being considered for modification, including potentially Crossroads architects or hosting platform specialists, if appropriate.

Based on the gathered requirements documented in a change request, Voyatek will come to the JAD session prepared with an initial solution that may be comprised of wireframes or story boards. This solution will be presented and discussed so that the North Carolina team has an opportunity to contribute to the design. A final design will then evolve during the meeting that defines the new, modified, or enhanced functionality or process with consideration given to WIC regulations, NC WIC policy, Participant Centered Services (PCS) design, and the most recent USDA requirements.

This process has proven to be successful because it allows our customers to participate in an interactive discussion with the design team and avoids multiple document exchanges to convey aspects of the design that may be difficult to convey in print format. Voyatek will capture notes during this meeting and deliver them to NC WIC as JAD Meeting Notes. These notes will form the basis for the formal version of the design and updates to the Detailed Functional Design Document (DFDD) and other system documentation as needed.

e) Transition-In and Transition-Out Communications

- 1. Describe the Vendor's process, frequency and format for meetings, conference calls and onsite visits during transition-in and transition-out phases, as well as status reports.*
- 2. Explain how the Vendor will provide a written summary, including but not limited to, the status of the Vendor's activities (completed since last update, new since last update, scheduled since last update, etc.), accomplishments, action items (those to be completed by the Vendor and by the State), and any new or changed risks or issues. Transition-In and Transition-Out communications will include such topics as:*
 - a. Tasks accomplished this period*
 - b. Deliverables submitted this period*
 - c. Outstanding tasks/deliverables*
 - d. Risk tracking log*
 - e. Outstanding problems, issues, and changes*
 - f. Function and architecture training agendas and action item lists for the application, batch, reporting, and portal areas.*
 - g. Minutes from source code and documentation walkthrough sessions*
 - h. Minutes from known defect walkthrough sessions*
 - i. Minutes from tool, hardware, and configuration walkthrough sessions that produce and install executable builds*

Because Voyatek is the incumbent vendor, the Transition-In period will not include transitioning to a new vendor and the focus of Transition-In will be the rehosting of NC Crossroads to the Azure cloud. As such, meetings and communications during Transition-In will be governed by the planning and cadence needed to support the rehosting activity. This is a very specialized activity, the details of which are provided in [Appendix E: Rehosting Implementation and Rollout Plan](#).

At contract Kickoff, the Voyatek product manager will present our proposed approach to rehosting and work with the NC WIC team to determine the proper format for meetings during Transition-In. Due to the special nature of the rehosting work and the careful collaboration that will be required with NC DIT, we recommend special rehosting weekly status calls throughout the

Transition-In period. Because there may be different NC staff in the rehosting meeting from the weekly M&E meeting, the Voyatek product manager will provide regular status updates on rehosting progress, accomplishments, plans, concerns, and risks as part of the regular weekly M&E status meetings also. Both rehosting and M&E activity will be presented in monthly status reports during the Transition-In period.

During Transition-Out, Voyatek will defer to the incoming vendor and the State to set the cadence for meetings because our role at that time will be one of support. We will report to the State on our accomplishments, plans, etc. as part of the normal monthly status reports until the completion of Transition-Out.

f) Maintenance and Enhancement Communications

Explain the Vendor's process, frequency, format, and timeline for Maintenance meetings, conference calls and onsite visits during Maintenance, as well as status reports. Explain the process for providing a written summary, including but not limited to, the status of the Vendor's activities (completed since last update, new since last update, scheduled since last update, etc.), accomplishments, action items (those to be completed by the Vendor and by the State), and any new or changed risks or issues. Maintenance status reports will be monthly no-cost deliverables submitted alongside the monthly M&E invoices, will be in addition to transition-in and transition-out communications, and will include such topics as:

1. Defects and defect resolution
2. Risk tracking log
3. Service Level Agreement (SLA) attainment
4. Change Request status

Throughout the M&E period of the contract, the Voyatek product manager will conduct weekly status calls and produce monthly written status reports. The weekly calls will focus on current activity, recent accomplishments, plans for the next week, current issues or recently identified risks that require discussion. The monthly written status reports will be no-cost deliverables that will be delivered in conjunction with the monthly M&E invoices. The monthly status report and invoice will be for the same period of performance with the status report containing the details of accomplishments to support the invoice. In addition, the status reports will include plans for the upcoming month, status of all open defects and change requests, the most recent plans for upcoming releases, updates to the Risk Tracking Log with highlights for any new risks identified, and measurements of Voyatek's performance against the service level agreement for the past month. When warranted, significant highlights of the monthly status report will be highlighted in the subsequent weekly status call.

g) Product Work Plan

Describe the Vendor's process, frequency, and format for providing and maintaining a Product Work Plan, that includes the following information:

1. Detailed product schedule including tasks required for Transition-In, the modification and deployment of Crossroads Change Requests and System Releases, and Transition-Out. Once the product schedule is approved by the State, any changes to dates and milestones will be approved by the State.
2. The product scheduling software to be used by the Vendor to generate the product schedule. Any proposed software will produce files in Microsoft Project Plan (MPP) data file format editable by Microsoft Project 365.
3. Work Breakdown Structure (WBS) with a graphic depiction that defines the tasks associated with the objectives for the entire scope of the contract. The WBS will be a decomposition of the work to be executed by the entire product team and indicate task dependencies along with start and end dates. The WBS will include all product deliverables, milestones, and activities at a level that allows the State to track progress towards completion.
4. Product tasks and deliverables that describe what is required to accomplish the work detailed in the WBS.
5. Note: Vendor may describe the Product Work Plan within the text of Vendor's proposal or provide a separate appendix. A final Product Work Plan will be due after Contract execution for the State's review and approval. The Product Work Plan will be updated with actual completion dates when final deliverables are accepted by the State.
6. The following is a tentative schedule of major milestones for an agile/waterfall hybrid approach.

(RFP Table 2 Crossroads Release Schedule omitted for brevity.)

Voyatek's draft Product Work Plan and Schedule addresses these requirements and has been included in our proposal as [Appendix C: Product Work Plan and Schedule](#).

h) Communication and Coordination Plan

1. Describe Vendor's Communication and Coordination Plan including the following information.
 - a. Vendor's communication approach, including events such as status reports, conference calls with various levels of State staff, webinars, onsite visits, etc.
 - b. All stakeholders involved with the product, including the State, the WIC EBT Provider, the Vendor and its subcontractors, and other major related parties.
 - c. How communications among and between stakeholders will be delivered and managed. This will include coordination among the units of the Vendor's product team, including product management, development, testing, and help desk.
2. Describe an overview of the communications approach that will be used with this product. The Communication and Coordination Plan description should include the following tasks:
 - a. Vendor will attend an annual onsite meeting to be held in Raleigh, NC.
 - b. Describe the Vendor's approach to hosting a weekly conference call or webinar as needed by the State of the Release Manager and State Subject Matter Experts to discuss topics requested by both the State and the Vendor.
 - c. Describe an action item tracking tool, compatible with Microsoft Edge, to be hosted by the Vendor and utilized by State staff.
 - d. Describe the Vendor's approach to hosting a collaboration web site, compatible with Microsoft Edge, to facilitate the sharing of documentation and other communication with various State staff.
 - e. Describe the software available to the Vendor to host webinars or other web conferencing. Vendor webinar software will not impose any licensing or location restrictions on the State.
 - f. Describe how communication will be coordinated with the WIC EBT Provider, and EBT FMNP Provider, for any activities related to these EBT interfaces.

Voyatek's draft Communication and Coordination Plan addresses these requirements and has been included in our proposal as [Appendix P: Communication and Coordination Plan](#).

i) Quality Assurance Management Plan

Describe Vendor's Quality Assurance (QA) Management Plan that includes the following information:

- 1. Describe the Vendor's quality assurance procedures as to how the Vendor will ensure that the Crossroads Product deliverables are of acceptable quality before they are delivered to the State. This includes describing the ability to advance the system clock of test environments as needed for life cycle testing.*
- 2. Describe the Vendor's approach to the various testing levels (i.e. development, Integration, and User Acceptance), in both for maintenance and enhancements, to ensure that the Crossroads system meets the State's expectations and requirements.*
- 3. Describe how quality of the QA Plan is measured, when quality checks occur and how corrective actions are determined and implemented.*
- 4. Both the State and USDA/FNS reserve the option to have a Quality Assurance (QA) Vendor or an Independent Verification and Validation (IV&V) Vendor provide third-party services for the Crossroads Product. Describe in the QA Plan the process for the Vendor to work with the third-party vendor, including hosting onsite visits to the Vendor's facilities, on recommendations and findings provided by the third-party.*
- 5. Describe the Vendor's approach in maintaining a repository of Regression Test artifacts, for use by the Vendor during the various testing levels and to meet the SLA under Table 3 - Service Level Agreement. This repository will be exported to the State upon request.*

Voyatek's draft Quality Assurance Management Plan addresses these requirements and has been included in our proposal as [Appendix D: Quality Assurance Management Plan](#).

j) Risk and Issues Management Plan

Describe a Risk and Issues Management Plan that includes the following:

- 1. Describe the Vendor's procedures for how the Vendor will identify, report, monitor, and recommend mitigation strategies for Risks and Issues.*
- 2. Identify who on the Vendor's Product Team is responsible for these activities.*
- 3. Describe a Risks and Issues Management Plan (that consists of a high-level overview of the Vendor's Risk Management processes).*
- 4. Describe the Vendor's approach in providing a Risk Matrix and Issues Log as product control deliverables throughout the term of the contract.*
- 5. Describe the Vendor's approach to perform a risk assessment and security assessment as defined by DHHS Privacy & Security Policy either through third-party or self-assessment on a three-year cycle (with a third-party assessment mandated every third year at the sole discretion of the State).*
- 6. Describe the Vendor's approach to document in the above assessments any Vendor (including subcontractors) intention to utilize offshore resources as stipulated in Attachment F.*

Voyatek's draft Risks and Issues Management Plan addresses these requirements and has been included in our proposal as [Appendix H: Risks and Issues Management Plan](#).

Voyatek is committed to meeting the Risk and Security Assessment requirements for Vendor critical systems and infrastructure as outlined by the State. We will conduct these assessments

every three years throughout the term of the contract, with the first assessment due during the Transition-In Phase. For a detailed example of our approach, please refer to section [c\) Security Vendor Readiness Assessment Report \(VRAR\)](#), which includes a sample report tailored to the architecture and hosting model required to support the Crossroads system.

k) Configuration Management / Release Management Plan

Describe a Configuration Management / Release Management Plan that includes the following information:

- 1. Describe Vendor's procedures for how the Vendor manages configurable items and maintains version control over deliverables, source code, installation tools, test scripts, etc.*
- 2. Describe the Vendor's Release Management processes, describing the Vendor's library system for managing North Carolina specific code and releases for defect remediation, including hotfixes.*
- 3. Describe how the Vendor will coordinate releases with the WIC EBT Provider.*
- 4. Describe the Vendor's process to adhere to the incumbent Release "x.x.x.x" nomenclature unless otherwise directed by the State.*
- 5. Describe how the Vendor will support up to three (3) different major releases of Crossroads installed in separate state environments, for example 1.42 in production, 1.43 in UAT, and 1.41 in a secondary test environment.*

Voyatek's draft Configuration Management / Release Management Plan addresses these requirements and has been included in our proposal as [Appendix J: Configuration Management / Release Management Plan](#).

l) Service Level Agreement

- 1. Describe Vendor's approach to comply with the following Service Level Agreement (SLA) provisions shown in Table 3 - Service Level Agreement, indicating agreement to the liquidated damages for each specific item for which a Service Level is established.*
- 2. Define the process for monthly invoice reductions for not maintaining the minimum threshold of acceptable service level, with carry over to subsequent months should cumulative liquidated damages exceed a single monthly invoice, or problems with service extend beyond a single month.*
- 3. The Vendor's approach should include a description of the format and frequency for reporting compliance.*

(RFP Table 3 Service Level Agreement omitted for brevity.)

A service level agreement is a vital component of Voyatek's commitment to NC WIC to maintain and operate the system so that NC WIC experiences minimal to no impacts to their business operation that is dependent on the Crossroads system. Our WIC Practice has a history of excellent quality service delivery and we do not anticipate having deficiencies in our work throughout the contract. However, despite the best focus and intention, sometimes mistakes can happen. Any deficiencies in Voyatek's performance against the service level requirements will be addressed with process improvements designed to prevent future shortcomings.

Voyatek is willing to accept the Service Level Agreements as detailed in RFP Table 3 and the associated liquidated damages for each of the eight service level criteria in the table. We recognize the importance of having specific, measurable, performance metrics to secure a

mutual understanding of expectations between NC WIC and Voyatek throughout the contract. However, Voyatek would appreciate the opportunity to discuss alternative Service Level Agreements with NC that would better align with the business objectives of the State. Voyatek is dedicated to delivering excellent service to North Carolina, as demonstrated by our work on the current contract. Strict SLAs can lead vendors to adopt a more cautious approach, focusing more on compliance rather than pursuing stretch objectives, innovation, and exceeding expectations. We would welcome the opportunity to discuss the best approach for the State that benefits North Carolina the most, working together as collaborative partners.

Across our portfolio of WIC projects, we monitor and regularly report on our performance against a variety of client expectations. We regard this as an important business practice to meet our clients' needs and expectations. Jennifer Saunders, the proposed Voyatek product manager, is a veteran of such project oversight. She will work with the NC WIC contract manager to maintain the monitoring and reporting processes to facilitate agreement on the SLA performance measurement process.

Jennifer will include SLA measurements in the monthly status reports. Any failure to meet compliance with an SLA will be accompanied by an explanation of why Voyatek missed the objective and what we will do to improve our performance in the future. In addition, the accompanying monthly invoice will reflect any liquidated damages, with carryover to subsequent months in the unlikely event that the liquidated damages exceed the monthly fee.

We pride ourselves on having an exemplary record of working collaboratively with our customers to resolve issues without getting into disagreements over severity level classification because of an SLA. We want to emphasize that having an SLA and liquidated damages to be assessed against us is not what drives us – rather, it is our desire to always provide exemplary service to our customers and we look forward to being able to continue our service to North Carolina.

m) Partnerships and Contractual Relationships

Describe Vendor's partnerships and contractual relationships when Vendor uses subcontractor(s) to fulfill the requirements of this RFP. Describe the types of service(s), contractual relationship and the term of the contract between Vendor and its subcontractor(s).

At the time of proposal submittal, Voyatek is not planning to use subcontractors in the services we will render for the resulting contract. At any time during the contract, should that position change, we will present our desired subcontractor and associated contractual relationship to the State for consideration. Please see Appendix M: Partnerships and Contractual Relationships for additional details.

3.5.4 Coordination with WIC EBT Provider / Interface with the EBT System

The State has awarded a separate Contract for WIC EBT in North Carolina whom the State refers to as the “WIC EBT Provider”. The Vendor and the WIC EBT Provider will fully cooperate and coordinate activities throughout the life of the current or future WIC EBT contract, including participating in any Transition-Out or Transition-In activities related to any change in WIC EBT contract, at no additional cost to ensure smooth operations and maintenance between the Crossroads and EBT systems.

a) Coordinate Interface with EBT

Describe and explain the Vendor’s process to coordinate with the current or any future WIC EBT Provider at no additional cost to the State to ensure that the two systems interface correctly (including providing diagnostic data to assist the WIC EBT Provider in resolving interface problems introduced by either party), and to make such Crossroads modifications as may be necessary to maintain a seamless interface on an ongoing basis for any future WIC EBT modifications that may be required. Describe how the Vendor will maintain an Interface Control Document (ICD) to document and provide the specifications for the interface points between the WIC EBT and Crossroads system.

As shown below, **Voyatek has worked with every WIC EBT provider to provide support for all versions of the WUMEI and has supported multiple projects with each of them.** We offer extensive knowledge of the NC Crossroads EBT interface including the original architect for Crossroads EBT function.

Table 3: Voyatek Experience Serving the WIC Community

State	MIS	Years of Support	Type of Support	Other Services	EBT Processor
Maryland	WOW	20	T&I / M&E	PedNSS/PNSS, Client Mobile App	Solutran
Virgin Islands	WOW	17	T&I / M&E	PedNSS/PNSS, Client Mobile App	Solutran
Michigan	WOW	15	T&I / M&E	PedNSS/PNSS, Client Mobile App	Conduent
Delaware	WOW	13	T&I / M&E	Client Mobile App	CDP/FIS
South Dakota	WOW	11	T&I / M&E	PedNSS/PNSS, Client Mobile App, Vendor Portal Client Portal	CDP/FIS
Florida	WOW	10	T&I / M&E	Client Mobile App	CDP/FIS
Indiana	WOW	9	T&I / M&E	PedNSS/PNSS, Client Mobile App	Conduent
Connecticut	WOW	8	T&I / M&E	Vendor Portal	Conduent

State	MIS	Years of Support	Type of Support	Other Services	EBT Processor
NATIONS (10)	WOW	7	T&I / M&E	PedNSS/PNSS, Client Mobile App	CDP/FIS
New York	WOW	6	T&I / M&E	Client Mobile App, Vendor Monitoring App, CARA (Vendor Investigations app)	Conduent
South Carolina	WOW	5	T&I / M&E	Client Mobile App, TeleHealth	Conduent
California	WOW	5	T&I / M&E	Client Mobile App	CDP/FIS
Illinois	WOW	4	T&I / M&E		Solutran
North Carolina	Crossroads	5	M&E	Client Portal	Solutran/CDP-FIS
Georgia	WOW	2	T&I / M&E		Conduent
Alabama	Crossroads	1	M&E		Conduent
Rhode Island	Crossroads	1	M&E	Cloud Hosting, SaaS	Conduent
Virginia	Crossroads	1	M&E		Conduent
West Virginia	Crossroads	1	M&E		CDP/FIS

Voyatek staff developed the Crossroads universal interface based on the 2012 WUMEI specification and will work with NC WIC to upgrade the EBT interface to current standards and to expand supported features as needed at no additional cost. Voyatek is the only MIS vendor to implement the 2020 Universal Interface, which improves transactional performance with a transition to JSON messaging. Voyatek has successfully upgraded Florida and California to the 2020 specification.

In addition, Voyatek is currently partnered with CDP to implement the upcoming 2022 WUMEI specification in both the WoW and Crossroads code bases. This project has two goals:

- Transitioning to the latest WUMEI version (2022) as mandated by FNS.
- Modernizing the EBT interface architecture and associated business processes to be cloud-ready, enabling seamless integration with both current and next-generation MIS systems.

WUMEI Modernization Project

This project also has major potential implications for the Crossroads MIS platform. The project scope includes many key features including:

- Implementation of all published Universal Interface message types
- Creation of cloud-ready containerized architecture
- Development of a modern web portal to manage UPC, NTEs, rebates, redemption processing, batch processing, and other functions
- Improved EBT functions for processes like voiding of benefits split between family members
- New abilities to delay sending future benefits to EBT cards until just prior to first date to spend providing WIC agencies more flexibility when responding to late arriving policy changes or disruptions to food availability
- Addition of an analytics platform for UPC, rebate, NTE, redemption, and other visualizations
- Full integration with existing Crossroads MIS systems

The project represents the starting point for large scale modernization to cloud optimized and responsive web technologies.

Voyatek has an excellent working relationship with North Carolina's current EBT provider and will work effectively to coordinate and manage EBT interface related activities.

Voyatek also maintains the following document "NC eWIC MIS Interface Specification Document (ICD) v1.5" which contains the relevant MIS to EBT interface details. This document was last updated by Voyatek for the transition of EBT services from Solutran to FIS/CDP and we will continue to maintain it for future changes to the EBT interface.

b) Coordinate Schedules and Testing with EBT

Describe and explain the Vendor's process to coordinate schedules and timelines to ensure that both systems maintain a seamless interface and the process to resolve any scheduling conflicts that might arise. Describe how this process will include internal testing between the Crossroads and WIC EBT systems prior to a Crossroads UAT to certify readiness for UAT.

Voyatek is the incumbent vendor currently maintaining the interface with the EBT system crossroads interfaces with today and is thus intimately familiar with schedules and timeliness necessary to allow this critical interface to function without interruptions.

Voyatek played a key role in transitioning North Carolina's EBT provider from Solutran to FIS/CDP, collaborating closely with CDP to establish the new operating environment.

For system enhancement involving new functionalities that impact the EBT system and interface, we will hold joint application development (JAD) sessions with NC WIC and the EBT Vendor, to obtain agreement and approval on configuration, SLAs, roles and responsibilities, and project timeliness for the hosting environment.

Voyatek's overall implementation strategy relies on our established business relationships and proven communications protocols/processes with all EBT vendors. This coupled with our release management processes will enable us to actively manage the end-to-end change deployment process; including version control, access to test facilities, batching changes for infrastructure or applications, oversight of system changes and confirming that post-implementation testing has occurred, and production documentation is completed.

In addition, daily operation involving both the on-line transactions, and batch files exchange, does require monitoring and coordination between Voyatek and the EBT provider, for effective troubleshooting and issues resolution. Voyatek monitors EBT processes daily and takes manual action when batch files fail, which has occasionally occurred with the redemption file.

For Voyatek's current collaboration with CDP to develop the first operational 2022 WUMEI interface, Voyatek is also developing the first automated EBT regression test to allow for testing of all universal interface functions. Voyatek has also developed an EBT simulator to allow EBT testing without being attached to an EBT processor in some scenarios. These tools are intended to greatly improve the ability of states to transition between vendors with little or no disruption. Voyatek's EBT platform is designed to allow for multiple vendors and WUMEI versions concurrently and to support transition between vendors. The system includes support for every current EBT function and includes management function to streamline operations that frequently result in EBT failures like benefit voids involving multiple family members.

c) Coordinate Training with EBT

Describe and explain the Vendor's process to coordinate training activities for UAT and deployment, as requested by the State due to a future modification of the interface.

The Vendor will be required to conduct all necessary Crossroads related consultation and training of the WIC EBT Provider staff at no additional cost to the State, in accordance with Section 3.4.2 e). Describe how Vendor will accomplish the foregoing.

Voyatek possesses extensive experience with North Carolina's Crossroads system and its EBT interface, having provided successful support over the past five years. Our team has frequently trained new North Carolina staff on processes directly and indirectly related to EBT. Cindy Kochersperger, the lead Business Analyst on the project and Voyatek's proposed BA for this initiative, has conducted training sessions on redemption and rebate analysis for both new and existing staff as required. This expertise proved invaluable during the formula shortage crisis in 2022, when numerous new formulas were rapidly integrated into the system.

Over the past decade, Voyatek staff have successfully executed ten new system implementations, which involved creating complete training materials, developing computer-based training modules, and delivering formal, just-in-time instructor-led training sessions. With extensive experience in conducting these training programs, we are well-equipped to educate

staff on new systems and functionalities. Voyatek will leverage this expertise to deliver tailored training for North Carolina staff, whether for onboarding new employees or updating existing personnel on system enhancements.

Voyatek will coordinate and conduct necessary Crossroads EBT-related training, which may become necessary as a result of future modification of the interface and agree to provide this service to North Carolina staff at no additional cost to the state.

The JAD sessions, together with the coordination and communication approach described above, allow the EBT provider management and staff to be an integral part of the development and implementation of any future modification which involves the interface. This approach, coupled with our extensive experience in designing and delivering training, will impart the knowledge and skills necessary to EBT provider staff to fully understand and use the modified system.

3.5.5 Coordination with EBT FMNP Provider

NC has moved FMNP to an EBT solution. Describe the Vendor's understanding and agreement that the awarded Vendor and the EBT FMNP Provider will fully cooperate and coordinate activities and training throughout the term of any EBT FMNP contract.

Voyatek has developed Farmers Market Nutrition Program modules for numerous states including several that utilize Solutran as their banking partner and helped several customers transition from coupon based FMNP solutions to electronic Farmer's Market solutions, both utilizing EBT and non-EBT methods.

Voyatek assisted North Carolina to update the coupon-based Farmer's Market Nutrition Program functions contained on Crossroads to interface with the Farm Market Direct system, the EBT FMNP system being managed by the current EBT Provider. Voyatek was actively involved in the requirements gathering, design, development, and rollout of the EBT FMNP solution with North Carolina and the EBT vendor. This involvement has provided us with an in-depth understanding of the code artifacts and processes involved in this implementation. Our team's expertise in this area enables accurate and efficient operation, addressing challenges that arise with precision thereby enhancing the overall effectiveness and reliability of this component.

Voyatek confirms that we will fully cooperate and coordinate with EBT FMNP Provider, activities and training throughout the term of any EBT FMNP contract.

3.5.6 Production and Non-Production Data Centers

a) Future Expansion

1. The North Carolina WIC Program has the potential to increase caseload quantities. Describe the Vendor's ability and methods to monitor State and Vendor system operations to make specific recommendations if additional processing resources and capacity is required to maintain acceptable processing requirements and timeframes.

2. Describe the approach the Vendor will take to procure additional Vendor system resources or capacity, and the time required to do so, should the need be identified.

During the Transition-In phase of the project, Voyatek will be shifting the hosting of the NC Crossroads system to the Azure cloud, as is described in detail in the [Appendix E – Rehosting Implementation and Rollout Plan](#). One of the benefits of cloud hosting is the ability to scale the infrastructure up (more power) and/or out (more servers) quickly and easily when needed. In the cloud, it is a process of configuration of the resources the system needs versus the data center process of specifying, requesting, acquiring, and deploying additional infrastructure. This is a part of the value proposition of hosting in a cloud environment.

Voyatek uses FortiSIEM to monitor and track components of the hosting environment including availability, processor utilization, memory, along with a wide range of other data points. These tools allow us to proactively identify issues and address them prior to their impacting program operations. Voyatek is proposing to increase application server capacity as part of the high availability configuration being proposed. This includes increases to reporting servers that will improve reporting capacity. Voyatek uses a tool called Terraform to manage cloud hardware using code rather than manual configurations. Terraform allows for high-speed analysis and deployment of infrastructure upgrades in cloud environments.

Voyatek technical staff have experience in preparing hardware and hosting requirements specifications for states as part of project implementation and maintenance activities. With each release of the system, our QA team revalidates that the Crossroads system performs correctly and efficiently with the current platform. This practice will continue after the transition to the Azure Cloud. Should the State's WIC caseload increase such that the Crossroads platform needs to be resized and scaled up, the Voyatek team will do that automatically, informing NC WIC of the change via the normal release and project status reporting process. This is a process that is performed across our WIC Practice for all WIC clients either in the cloud, in our hosting environments, or in collaboration with state personnel where the system is hosted in a state data center.

b) System Performance

1. Performance testing activities will be described in the QA Plan. Describe the Vendor's approach to performance testing the system after modifications for maintenance and enhancements in their internal test environments.

The QA team executes System Test in a dedicated test environment that mimics production as closely as possible in terms of configuration and security. The System Test environment contains a full data snapshot (rather than partial data sets used in other test phases) that supports parallel functional and technical system and performance testing. With each release of the system, the Voyatek QA specialist validates the system performance will not be degraded by any change in the release. There are a variety of techniques and tools we use to do this depending on the nature

of the enhancements or changes in the release. [Appendix D: Quality Assurance Management Plan](#) includes further details on our approach to system performance testing and management.

2. Describe Vendor's approach to monitoring system operations daily and making necessary mutually agreeable adjustments to maintain peak operation efficiency so that system users are not adversely affected. Describe the type of automated and manual systems that will be used by the Vendor if requested.

Voyatek currently supports the day-to-day operations of WIC systems for many state agencies (including North Carolina) with participation ranging from a few thousand to over a million participants, on both web-based and smart client platforms. There are unique challenges that present themselves in supporting such a wide range of systems with regards to coordination, communication, environment configuration and core technical expertise. We provide excellent support by assisting with troubleshooting of issues in the hosting environment and by assisting local clinic IT with troubleshooting of issues experienced by the clinic staff. We employ a four-step methodical approach:

1. Identify the Symptom – document what is being experienced by the user and try to determine specifics from problem statements shared by end users
2. Determine the Root Cause – based on the symptom(s), investigate by performing a root cause analysis to determine the root cause of the issue
3. Plan the Solution – develop a plan for resolving the issue and determine the appropriate course of action based on the criticality of the problem
4. Implement the Solution – develop the solution and implement it in the target environment with the knowledge and approval of the State

The correct operation of the system is highly dependent on the resources available to it. Monitoring these resources such that they are operating within thresholds is an important aspect maintaining continuity of operations. Currently, the Voyatek Crossroads support team works in conjunction with NC's Department of Information Technology (DIT) that provides hosting for the Crossroads system to understand how the system is performing and to provide recommendations as needed for improvements or adjustments as the need arises and as the system evolves through maintenance. During Transition-In of the new contract, as we migrate the system hosting to the Azure cloud, we will also transition the system operations and monitoring to be performed by the Voyatek team.

Voyatek will leverage the automation capabilities of FortiSIEM, integrated with Azure Monitor, to continuously monitor and optimize daily system operations. This approach maintains peak operational efficiency while preventing adverse impact on system users. Through automated data collection from Azure Monitor, along with logs, performance metrics, and event data, FortiSIEM provides visibility into resource utilization of critical system components, including virtual machines, databases, and batch processes. FortiSIEM's real-time event correlation and automated anomaly detection, combined with Azure Monitor's metrics, enable the identification

of performance issues, security risks, or inefficiencies as they arise. FortiSIEM allows the configuration of alerts and pre-defined workflows that notify support personnel when anomalous behavior is detected, enabling them to address issues promptly before they affect users. Voyatek will assess system performance trends, using insights from both FortiSIEM and Azure Monitor to make necessary adjustments. These adjustments may involve scaling resources, reconfiguring systems, or troubleshooting potential problems to maintain system efficiency.

3. Describe Vendor's approach to performing mutually agreeable timely database tuning to keep the databases running as efficiently and effectively as possible. Describe the type of automated and manual systems that will be used.

With the experience Voyatek has gained supporting enterprise level systems, we have learned that in most cases, application performance can be directly correlated to database performance. The application can become overwhelmed or unavailable if the database does not respond as it should, affecting its reliability.

Database performance is generally a factor of resource allocation, database parameter settings, and the amount of data that the database must query. Even the best configured databases, if not closely monitored and regularly tuned, can suffer from performance degradation over time. As NC caseload grows and more data is ingested into the system, or as software modifications are introduced, memory, CPU, and disk allocations must be closely monitored to validate that the database is not being stressed for the want of resources.

Voyatek's practice is to review SQL query performance on a regular cadence. If poorly performing queries are identified, the DBA will evaluate the situation and work to either adjust database parameters or collaborate with the development team to formulate a solution.

Voyatek has experience with optimizing database performance working with large WIC systems, including the NC Crossroads MIS. The Crossroads database has been performing consistently and well for many years as Voyatek has maintained the Crossroads system, working with the NC DIT staff. As we transition the system to the Azure cloud, the Voyatek team will review recent database performance metrics with the DIT operations team which will then be factored into the database tuning in the cloud. Following the transition to the cloud, we will utilize the Azure monitoring suite to identify long-running queries or other database performance issues that require tuning adjustments.

In addition, with each release, Voyatek software development and database administration staff will review recent database performance, evaluate the changes being implemented in the upcoming release, and generate recommended changes for consideration to keep the Crossroads database performing at peak efficiency. Any recommended changes will be discussed with NC WIC prior to making the operational changes in the database.

As part of the transition to Azure SQL Managed Database, Voyatek anticipates updating the North Carolina Crossroads database to the most current version of SQL Server. This will improve performance and provide the best experience going forward. Voyatek has successfully updated Rhode Island's SQL Server as part of their Azure upgrade process.

4. Describe Vendor's approach to adhering to the following expected page load and/or response times:

- a. An average response time of 1-3 seconds for basic transactions such as insert, update, delete, and queries from a single table.*
- b. 5-25 seconds for "complex transactions" – Complex transactions are defined as those that require:
 - i. Data requests from the application database or data store;*
 - ii. Dependencies on application work flows or back end processing;*
 - iii. Interfaces with external applications or web site.**
- c. 5-200 seconds for generation of ad-hoc reports, depending on complexity and size of each individual report. These reports are generally created using predefined data queries which are optimized for performance. These reports are also generally collecting smaller subsets of data versus more complex analytical reports.*
- d. 5-30 minutes for generation of complex analytical reports. These types of reports generally require back end processing or complex data queries. Analytical reports are generally built in real time based on queries created by the end user, where the queries are not optimized for performance. These reports also tend to require larger subsets of data than ad-hoc reports.*

Voyatek understands that reasonable response times are essential to a functional system. During release testing, our quality assurance staff will conduct applied performance tests to verify response time criteria are met while the system is under load. We will provide the support necessary to provide the above response times throughout the maintenance and enhancement contract period.

5. Describe Vendor's approach to execute Performance testing activities annually (by a mutually agreed upon date) in the Vendor's technical environment, testing Crossroads under full-load and no-load conditions during normal and peak performance periods.

- a. Describe Vendor's proposal for providing an annual draft Performance Test Plan to the State for approval prior to start of each annual performance test that addresses the criteria listed above.*
- b. Describe the Vendor's approach to evaluating the need for performance testing Crossroads in its internal test environments after the completion of maintenance and Change Request modifications.*
- c. Describe how Vendor will advise State staff on Vendor Performance Test Scripts to perform automated tests on Crossroads as specified by a Test Case.*
- d. Describe a Performance Test Results Report that outlines an executive summary and the detailed documented output of the execution of every Test Case for performance testing, which the State will review and approve. For every Test Case, actual test results will be documented, including any necessary re-testing required by the State prior to the delivery of the applicable release for UAT.*

As we transition Crossroads into the Azure cloud, Voyatek technical staff will meet with DIT staff to review recent load tests performed by North Carolina and request copies of the load testing procedures and scripts. Upon transition to the Azure cloud, Voyatek will perform annual performance testing by a mutually agreeable date which will be established during project kickoff. During these annual load tests, we will utilize the most recent North Carolina load test code with necessary updates for the cloud platform. The testing will be conducted in the testing environment. This environment will not be scaled to match production workloads but will be tested for proportional performance expectations.

In advance of the annual test, the Voyatek team will prepare and present to the State our draft Performance Test Plan which will describe the tools and methodology to be used during the performance tests, how results will be recorded, findings established, and results shared with the State. In addition, the plan will describe Voyatek's approach to assessing the need for performance testing as part of our standard release testing process. At times, system enhancements can create modifications to the database or data layers in the system that may require specialized tests to confirm system performance to standards.

Upon review and approval of the Performance Test Plan by the State, testing will commence as scheduled. The testing process will yield a Performance Test Results Report which will report each test case undertaken in the testing process, the methodology performed for the test, the results captured, any retesting that was needed, and any recommendations for the State's consideration. The Performance Test Results Report will be delivered for the State's review and the Voyatek team will be available to discuss any aspect of the report as needed.

As for automated testing, the Crossroads XAML application, in general, is not testable using current automated testing tools due to the smart client architecture of the system. Voyatek does utilize test automation for web-based systems as they are developed. For example, we are currently using Playwright to develop automated tests for our EBT modernization project. Playwright tests are performed each time a new version of the software is deployed to development and test environments.

c) System Security at Vendor Facilities

The Vendor will be responsible for providing a comprehensive security and vulnerability program that meets applicable State and Federal requirements to protect the integrity and confidentiality of program data. This program will include administrative, physical, technical, and system controls.

1. Describe Vendor's Security and Vulnerability Plan for the following:

a. The location and description of the controls at each of the physical Vendor facilities where contract-related activities occur to protect data from unauthorized use and access, such as entrance security, use of access cards, restricted access areas, Closed Circuit Television (CCTV), fire protection, etc.

b. The types of controls, for both Vendor local and cloud-based solutions, over the development and testing environment hardware and software to protect data from unauthorized use and access, such as communication

access controls, user identification and authentication, system access and audit controls, transaction communication controls, discretionary access controls, separation of duties, data destruction procedures, etc.

c. The virus and malware controls to protect data from unauthorized use, access, contamination or corruption.

d. Vendor's plan for the event of a suspected or confirmed Breach, Cybersecurity Incident, or Significant Cybersecurity Incident involving Crossroads or the State's Confidential Information, at the Vendor's own expense:

- i. immediately report such Breach or incident to the DHHS Privacy and Security Office at <http://www.ncdhhs.gov/about/administrative-divisions-offices/office-privacy-security> (or, if website is unavailable, fax to 919-733-1524) within twenty-four (24) hours after first discovery, as well as to the Contract Administrator and DHHS Release Manager;*
- ii. investigate such suspected or confirmed Breach or incident;*
- iii. provide a remediation plan, acceptable to the State, to address the Breach/incident to prevent any further Breaches/incidents;*
- iv. conduct a forensic investigation to determine what systems, data and information have been affected by such event;*
- v. cooperate with the State, and any law enforcement or regulatory officials, credit reporting companies, and credit card associations investigating such Breach/incident.*

e. The Vendor will update the plan throughout the life of the Contract as industry standards change, new State and/or Federal requirements are issued, or new security or vulnerability concerns are discovered.

Crossroads hosting will be maintained within the Microsoft Azure Commercial Cloud. The Azure cloud is FedRAMP certified and maintain current SOC 2 audits. All access to facilities meets NC requirements and is documented by Microsoft. Voyatek utilizes Microsoft Defender and CloudStrike on all hosting infrastructure for anti-virus protection. Voyatek has an incident response and reporting policy that coordinates communication in the event of a security event in accordance with NC requirements.

Implementing robust security controls is an integral part of Voyatek's software development strategy. We systematically integrate a multi-layered approach to protect systems against potential threats. Authentication mechanisms are diligently enforced, allowing only authorized personnel to gain access to sensitive areas of the software. Authorization protocols are meticulously designed, restricting privileges based on roles and responsibilities. Stringent encryption practices are embedded into data transmission and storage processes, safeguarding information from unauthorized access. Regular vulnerability assessments are conducted, providing insights into potential weaknesses, and enabling timely remediation. Public facing websites and applications are particularly susceptible to attacks and threats, therefore it is crucial to exercise heightened caution to implement protective measures for these applications.

Voyatek's extensive experience over two decades involves managing systems primarily hosted in state-managed data centers. We understand the critical importance of security and compliance with state requirements. Voyatek enables the security, confidentiality, and processing integrity of the systems and data we oversee through robust internal controls that have been designed with care and have been successfully reviewed through independent audits by accredited third-

party auditors. These audits, which are conducted under the System and Organization Controls 2 (SOC 2) Type 2 examination framework (AT-C 105 and AT-C 205), reflect our commitment to maintaining high standards of security and data integrity, providing our clients with a reliable and trustworthy service.

The Security and Vulnerability Plan is provided in [Appendix G: Security and Vulnerability Plan](#). This plan addresses all aspects of the above security requirements. Voyatek has completed a Security and Vulnerability plan for the North Carolina Connects CACFP system hosted in the Azure cloud. That plan has been provided as a draft baseline for the Crossroads plan. Due to the technology differences between the projects, many updates will be required to map each component used by Crossroads. However, the primary approach, Voyatek policies, procedures, and controls will be consistent between projects. Voyatek anticipates being able to provide an updated plan early in the transition-in period.

In addition, Voyatek is providing a complete copy of our 2024 SOC 2 Type 2 audit report as [Appendix Q: SOC 2](#) which demonstrates our compliance with evolving security standards. To meet SOC 2 standards, we maintain a library of policies, procedures, and evidence related to security and vulnerability practices.

2. Describe the process that will be used by the Vendor to notify individual(s) or parties affected by a security incident(s). If any applicable federal, state, or local law, regulation, or rule requires the State's or the Vendor to give affected persons written notice of a Breach arising out of the Vendor's performance under this Contract, the Vendor will bear the cost of the notice ("Notification Related Costs"). Providing notice to affected parties will include the following:

- a. The date of the notice.*
- b. The reporting entity's name and contact information so that affected individuals can obtain additional assistance or information.*
- c. A brief description of the data breach incident in general terms.*
- d. The date of the breach, if unknown, the approximate date or date range of the breach.*
- e. The categories of personal information at issue.*
- f. A brief description of the actions taken by the Vendor to contain the breach and protect data from further unauthorized access or use.*
- g. Advice on actions affected individuals should take.*
- h. Contact information for national consumer reporting agencies.*
- i. Recommendations for affected individuals to protect themselves. For example, reviewing account statements, monitoring free credit reports, or subscribing to credit reporting services as stipulated in Attachment B.*

Voyatek has reviewed and accepts the above list of data elements to be included in any Breach notifications. In the unlikely case that a security lapse should allow a Breach arising out of our performance under the contract, we will engage and work with an outside counsel experienced in responding to security incidents to comply with applicable laws and regulations governing notice and notification related costs.

3. Describe an overview of the security protocol that will be used with this product, including a statement that the protocol complies with all standards and specifications, as listed in this RFP. Describe any security issues that may have occurred at the facility that will be used for North Carolina development and testing processing in the past three (3) years and how they were mitigated.

Within the scope of our Managed Services Network Operations Center (NOC), a key aspect of our capabilities lies in delivering and sustaining advanced remote diagnostic functionalities, coupled with proactive and reactive troubleshooting activities for seamless system maintenance. Having deep experience with industry-standard tools such as Datadog, Dynatrace, FortiSIEM, and New Relic allows the NOC to remotely monitor and analyze system health with precision. This proficiency empowers us not only to identify potential issues proactively but also to initiate troubleshooting measures swiftly, minimizing disruptions and ensuring continuous operational excellence.

Voyatek utilizes FortiSIEM extensively on all production environments hosted by our Managed Services organization. FortiSIEM is a top tier security operations center (SOC) and network operations center (NOC) application provided by the security company Fortinet that combines feature sets of both Network Monitoring Products and SIEM products. It is highly flexible and can be used to monitor any system that can provide logs and other information to the FortiSIEM system. FortiSIEM brings together visibility, correlation, automated response, and remediation in a single, scalable solution. It reduces the complexity of managing network and security operations to effectively free resources, improve breach detection, and prevent breaches.

Aligned with the highest industry standards, our focus on providing cutting-edge remote diagnostic capabilities is a testament to our commitment to technological leadership. Regular updates and optimization efforts within the NOC ecosystem are guided by industry best practices, ensuring that our remote diagnostic tools remain at the forefront of efficiency and effectiveness. As a result, our Managed Services NOC stands out as a reliable partner capable of navigating dynamic technological landscapes, offering clients resilient and efficient systems supported by state-of-the-art remote diagnostic solutions.

In the past three years, there have been no security issues in the on-premises development and testing environments for NC Crossroads. These environments are operated by Voyatek in our TierPoint Data Center.

4. Describe the approach for Vendor to continue to comply with data retention and notification about a breach of data until the data retention period has expired and the data has been destroyed or purged and the Vendor has provided written certification of such destruction or purge to the State.

Following the contract and as part of Transition-Out, Voyatek will continue to comply with all data retention and breach notification requirements and processes until the Transition-Out is completed and Voyatek has destroyed all State data and provided written certification of such data destruction or purge to the State.

5. Describe the Vendor's process for conducting vulnerability scanning and testing against the Crossroads system installed in internal Vendor environments and Vendor-managed State production and test environments, including all web portals, with a minimum of publishing vulnerability results to the State as part of the Security Assessments stipulated in Table 1 – List of Product Deliverables.

Voyatek has adopted commercially available and industry standard tools for conducting vulnerability and penetration testing for platforms and environments that we host. We utilize The Micro Focus' security suite which includes Fortify on Demand (FOD) and WebInspect. FOD is a cloud-based application security testing (AST) solution which enables organizations to identify and remediate security vulnerabilities in their applications by providing dynamic application security testing (DAST) and static application security testing (SAST) capabilities in an on-demand, scalable environment. WebInspect, also a dynamic application security testing (DAST) tool, is designed to evaluate the security of web applications and service endpoints while providing customizable workflows and integration with a variety of authentication schemes.

Upon transitioning North Carolina's production and test environments to the Azure cloud, Voyatek will include those environments in our scanning for the Crossroads systems. Our scanning includes all web access points including portals. Upon

6. The State and Vendor may perform vulnerability scans against all Vendor-managed cloud servers. Describe how any vulnerabilities identified by the State or by the Vendor, that are specific to the design of Crossroads, will be corrected by the Vendor in a timely manner at no additional cost to the State.

Voyatek understands that the State may perform vulnerability scans against the Voyatek-managed cloud infrastructure at any time. Voyatek performs (or contracts for) regular vulnerability scans and tests as part of our normal security management protocols and welcomes North Carolina's additional testing whenever the State chooses to do so. When the State performs such scans, we request a copy of the assessment results even if there were no apparent concerns so that we may review the findings with the State and catalog the findings as a part of project management and security best practices. In the case that the State finds a weakness or vulnerability, we will assess the best way to correct the deficiency, discuss the approach with the State, and make the needed adjustment in a timely manner at no additional cost to the State.

7. During the execution of the resulting Contract, the Vendor will notify the Contract Administrator and DHHS Crossroads Release Manager within twenty-four (24) hours of any contact by the federal Office for Civil Rights (OCR) received by the Vendor.

Voyatek affirms that we will notify the DHHS Contract Administrator and Crossroads WIC MIS Release Manager within 24 hours of any contact with Voyatek by the Federal Office for Civil Rights.

8. Describe process and timelines for the Vendor to comply with any State requests for information related to a breach, including but not limited to: root cause analysis, impact, mitigation strategy, technology involved, and timing.

In the unlikely event of a breach of data in the cloud facilities and environments managed by Voyatek, we will promptly comply with all State requests for information related to the breach, including but not limited to our root cause analysis, the technology utilized, the timing of the breach, the impact to North Carolina and Voyatek, and the mitigation strategy to minimize the damage. The Voyatek product manager will be the primary point of contact who will work with our cloud team, our managed services leadership, Nutrition Practice leaders, and the NC WIC team to be sure necessary information and mitigation steps are communicated to the State on a consistent cadence throughout the breach response process. Voyatek will document and log all related events as a part of our breach management process and provide full documentation to the State as soon as practicable.

d) Disaster Recovery at Vendor Facilities

The Vendor will be responsible for providing disaster recovery services and staff facilities with this product that minimizes production system downtime to no more than one (1) continuous hour of total service disruption in the event of a disaster. Describe Vendor's Disaster Recovery and Contingency Plan. The Vendor will update the Plan throughout the life of the Contract as necessary. Describe Vendor's Disaster Recovery and Contingency Plan for the following:

- 1. A description of an evaluation of the types of disasters that may affect the ability of the Crossroads development, testing, or Help Desk staff facilities to operate;*
- 2. A description of the plan to mitigate the effect of such disasters;*
- 3. A description of the disaster recovery facilities that will be used in the event of a disaster;*
- 4. A description of the criteria for determining when the Plan will be invoked, the staff that will be involved, and the timelines for providing notification to the State;*
- 5. A description of how the environments will be restored once the disaster situation has been resolved;*
- 6. A description of how and when the Disaster Recovery Plan will be tested.*
- 7. A description of an overview of the disaster recovery facilities and procedures that will be used with this product.*

The Disaster Recovery and Contingency Plan is provided in [Appendix F: Disaster Recovery and Contingency Plan](#). This plan addresses all requested elements of Disaster Recovery at Vendor Facilities and has been updated to reflect the transition of hosting to the cloud, which is required to be completed during the Transition-In phase of the project.

e) System Requirements for User Hardware and Software

Describe how the Vendor will maintain descriptions in the existing System Documentation of the minimum hardware configurations, including operating systems and web browsers, required to access / operate the System from the computers being used at the State Office level and the clinic level, so that the State can verify that existing hardware / software used by staff is sufficient or whether an update is needed prior to release deployment.

Maintaining accurate and current system documentation is an essential activity for all the WIC systems we maintain because state agencies rely on that documentation for a complete understanding of their system(s). For the NC WIC Crossroads system, Voyatek updates the appropriate system documentation as needed for every release based on the specifics of each

release. The primary focus is typically on the Detailed Functional Design Document (DFDD) as that deliverable describes the functionality of the system at a granular level. And we also update the Data Dictionary, Report Definition Documents (RDDs), test scripts, and the Crossroads Configuration Plan (where the minimum hardware and software specifications are found) based on the content of each release.

The minimum hardware configuration required to operate Crossroads typically does not change from release to release. The Voyatek QA team assesses system performance with each system release as a part of our release management process. Should a given release incorporate functionality that might create a potential change in the minimum hardware configuration and/or the software stack required to support Crossroads, the Voyatek team determines that early in the release process so that the change can be discussed with the State team to determine if the change will create any issue for the inventory of workstations currently deployed for Crossroads. In such a case, not only will we update the system documentation, but we will work closely with NC WIC to confirm workstations in the field will be ready when the release is ready for production deployment.

3.5.7 Help Desk Services

General Help Desk Specifications

Describe the Vendor's process for providing system support services to State WIC Office staff (via an unlimited toll-free telephone number, email, and issue reporting system). Customer service will be provided by a facility with staff physically located in the continental United States, as specified in Attachment K. Federal and Other State Specifications.

Describe Vendor's Help Desk Plan that details how the Vendor will provide customer support services and describe the below elements.

- 1. Describe the Vendor virtual capabilities that will allow State staff to share workstation images real-time with Help Desk staff.*
- 2. Describe how the Vendor will log and will develop a library of common debugging steps to assist with the resolution of issues (including hardware issues) or the documentation of more complicated issues that get referred to development staff for further research.*
- 3. Describe the Vendor's escalation protocol for handling all calls to ensure that critical calls are handled in a timely and appropriate manner. Include in the explanation a process and a timeline for notifying the State when the determination is made that an issue (critical or non-critical) appears to be system-wide that affects multiple users.*
- 4. Describe the process and frequency of training provided as new help desk staff are hired and/or as additional modification are made to the System prior to the release deployment of such modifications so that staff are fully knowledgeable of the changes.*
- 5. Describe the process of how the Help Desk staff will have access to management and/or technical resources so that issues can be handled in a timely and appropriate manner.*

6. Describe the process of how the Help Desk staff will request and maintain access to the production and test/training environments so that the Vendor can research server and application issues on a real-time basis.

7. Describe the process for tracking calls and Help Desk activities that enable the Vendor to monitor and track the volume of calls so that staffing levels may be adjusted accordingly as call volumes dictate.

8. Describe the process to capture and determine common issues that might indicate a system-wide defect, an area where a System modification may be needed to enhance System use, or the need for additional user training.

9. Describe the types of reports that are available that summarize various Help Desk activities and statistics for internal use and for State use. Include sample reports with the response.

10. Describe and explain how the following performance standards for call handing will be met:

a. Calls will be answered by live staff within one (1) minute.

b. For a critical statewide production down issue reported by any State staff, the Vendor will provide written acknowledgement to the reporting State staff, the Contract Administrator, and the DHHS Release Manager within fifteen (15) minutes that the appropriate Vendor staff are working on the issue.

Help Desk Support for State Users

The Vendor will provide the State WIC Office with technical assistance for Crossroads related issues during normal clinic business hours.

Describe how the Vendor will provide the following services and tasks under this category in 1 through 4 below. For each item, explain how each service and task will be fulfilled.

1. This assistance will be with live staff via telephone, email, and issue reporting system.

2. Normal business hours are defined under Attachment B. Federal or Vendor holidays not observed by the State are considered normal business hours. The State observed holiday schedule is available at the NC Office of State Human Resources website.

3. Providing email support to use for non-essential issues. All emails will be responded to within one (1) Business Day of receipt. If the issue cannot be resolved within that time frame, a reply email is still required within that time frame to acknowledge receipt and to provide a timeline for resolution.

4. Providing an adequate number of qualified staff thoroughly trained in customer service, general technical skills, and specific knowledge about the Crossroads System to handle a minimum of twenty-five (25) issues per quarter.

Across our WIC customer base, Voyatek provides various levels of help desk support as required by each client. While we offer all levels of support, we have an appreciation for states that prefer to provide their own initial Help Desk support (often called Level 1) like NC WIC because the State team is always best equipped to provide guidance on specific State policies and procedures.

Voyatek will provide help desk support to the NC state office staff to help maintain the day-to-day operations of the NC WIC Crossroads MIS inclusive of components, interfaces, and data. We will do this utilizing our team of Crossroads subject matter and technical experts, all of whom are located in the continental United States. This team is the same team that NC WIC has come to know and trust over the past six years. **Our team's ability to understand and diagnose problems**

quickly and efficiently to allow for minimal disruption to the NC clinic and state staff is a significant part of the value proposition that Voyatek offers to North Carolina.

We provide direct contact information for our Crossroads product management team members so that NC WIC has the most efficient support for the state office staff. In addition, we maintain a central WIC help desk with operating hours that correspond to North Carolina's normal business hours and with a dedicated unlimited call, toll-free phone number for NC WIC staff to receive prompt support for reported issues. Our help desk team records reported issues in their issue management system and contacts our Crossroads support team to initiate a timely and efficient response. These two methods of reaching our Crossroads support team enable the NC WIC team to have their questions and issues addressed promptly. In addition to phone calls, for lower priority issues, the NC WIC staff may opt to send emails directly to our team. The Crossroads product team has a demonstrated track record of being responsive and efficient in tracking and resolving issues for NC WIC. They have the knowledge and capability to handle a minimum of 25 issues per quarter as required by the RFP.

The Voyatek teams use Azure DevOps to organize and manage most aspects of our technical support, and this includes logging of all help desk tickets for the NC Crossroads product team to address. We will continue to provide access to DevOps for the NC WIC state office staff to allow them to view, update, and add defect information directly into Azure DevOps. All issues that were initiated by a phone call or email are logged into DevOps by the Voyatek team. Tickets needing immediate attention are marked as urgent and escalated to a Voyatek team member.

[Appendix N: Help Desk Plan](#), addresses our detailed approach to meeting the General Help Desk Specifications in the RFP and describes elements such as:

- How we use Microsoft Teams for conference calls and to support multiple people as needed to triage a problem and, when necessary, share screens to help our team understand what the NC WIC staff is seeing and experiencing.
- How we use Azure DevOps for cloud-based tracking of all help desk issues with direct access provided to the NC state office staff. DevOps categorizes issues based on priority, provides recommended steps to resolve common problems, and supports escalation of issues as needed via prioritization.
- Our approach to issue escalation and communication when issues are realized to be affecting a wide group of users. This includes recommendations of changes to the system for NC WIC's consideration as adaptive or perfective enhancements and/or additional training for WIC staff.
- How we train new team members and support them as they learn Crossroads and our protocol for supporting NC WIC. This includes changes in system functionality in advance of its release to the NC WIC staff and users.

- Our approach to environment access management for our team members based on their experience and responsibilities.
- Detailed procedures for how NC WIC staff can interact with our experienced team members easily and efficiently, including access to the Voyatek management team whenever needed.
- How we will manage our support to the State's service level standards and the reporting metrics we will provide to support our adherence to those standards such as a one-minute call response time and 15-minute written response time for statewide production down issues). If an issue appears to be system-wide that affects multiple users, the issue will be reported directly to the Voyatek product manager who will then notify the State Contract Administrator and DHHS Crossroads WIC MIS Release Manager of the issue and what is being done to mitigate and resolve the issue. The call by the product manager will be followed with an email to the State with a full description of the issue, what caused it, steps taken to mitigate the impact and the final resolution.

3.5.8 Issue Identification and Correction from UAT and Production

The Vendor will be responsible for providing the following services and tasks under this category after contract execution. Describe Vendor's proposal for providing a draft UAT Readiness Report prior to the start of each UAT release and describe how Vendor will address the elements below.

a) Comprehensive Testing

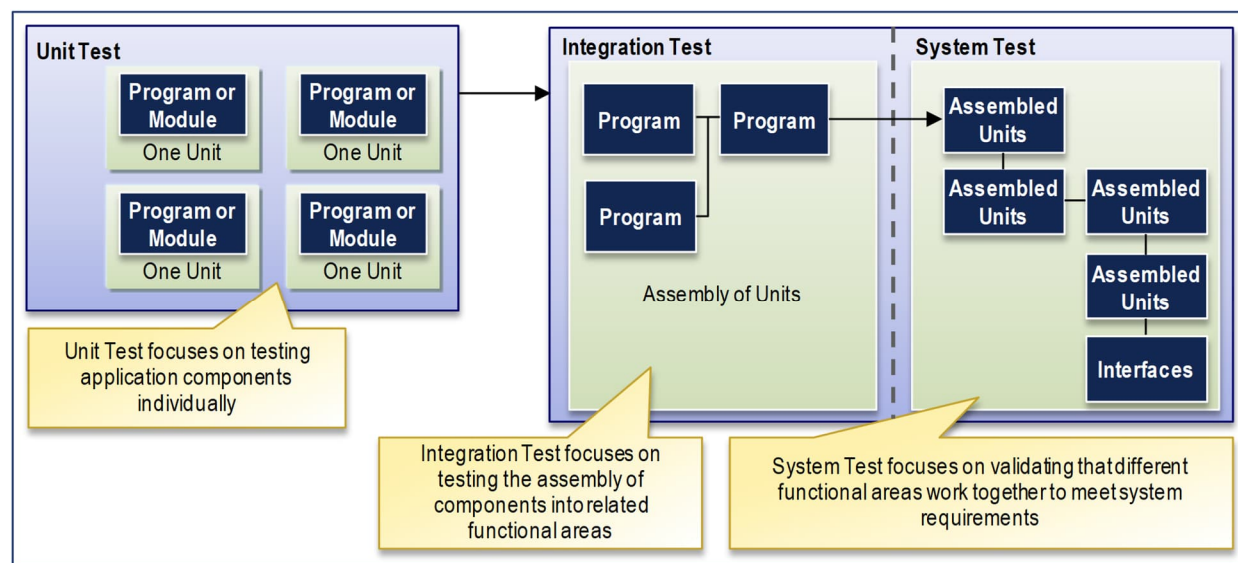
The UAT Readiness Report will describe how the Vendor provided and supported end-to-end testing of the Crossroads System functionality with comprehensive financial testing until the State was satisfied the System is working properly in accordance with requirements. Testing will involve issuing benefits, redeeming benefits, running reports (such as participation, FNS-798, Not-To-Exceed (NTE), and rebate invoicing), and any other functions requested by the State.

While EBCI is a separate state agency, Crossroads supports EBCI as a local agency within NC. The ability to separate out EBCI redemptions will be maintained in the QA Management Plan and demonstrated in testing for the UAT Readiness Report until the State is satisfied the System is working properly in accordance with requirements. Testing will involve issuing benefits, redeeming benefits, running reports (such as the rebate report), and any other functions requested by the State.

The draft UAT Readiness Report generated after contract execution will include these elements from the QA Management Plan:

- 1. The types of testing to be performed;*
- 2. The organization of the test team and associated responsibilities;*
- 3. Test database generation;*
- 4. Test case development;*
- 5. Test schedule;*
- 6. Documentation of test results Describe Vendor's process for creating a Test Plan for use in satisfying UAT Readiness.*

Voyatek's proven testing approach defines coordinated testing activities that span the System Development Life Cycle (SDLC) to validate the output of requirements, design, development, and implementation. The Test Team engages with the State and other project sub-teams early and often and encourages active participation and feedback throughout the test effort.



OIE-12.039

Figure 3: Voyatek Team Test Phases

Voyatek provides a detailed summary of test results in an agreed upon format for each test phase. This summary documents requirements traceability/coverage, test script pass/fail results, and a listing and disposition of each identified defect. The table below provides an overview of each test phase executed per release. We work closely with the State stakeholders during each test phase to identify defects early in the test process to minimize rework and achieve quality targets.

Table 4: Voyatek Test Phases

Test Phase	Description	Scope
Unit Test	- Evaluates each logic branch or decision point within a component - Executed by the Development team - Subject to Peer Review by Development team lead/members	Individual software component
Integration Test	- Confirms communication / integration of related modules - Executed in cooperation with the Development and Testing teams - Documented as Subsystem Integration Test within the Testing Plan - Includes interface and regression testing and may span applications within the system	Related modules in a functional area

Test Phase	Description	Scope
System Test	- Tests end-to-end business processes that span the application functionally/technically - Executed by the Test team; Peer reviewed by Test/Technical/Design teams - Includes interface testing to internal and external systems - Addresses conversion/legacy data and regression testing	Complete system
Performance Test	Consists of three unique testing cycles executed concurrently with System and repeated during UAT by the Test /Technical teams: - Performance testing subjects a server to load conditions that would be realized in the production environment including load balancing - Volume testing determines 125% of the estimated maximum number of concurrent users / transactions can be supported by the application including load balancing - Stress testing validates the application's upper thresholds, stability and reliability over time including data management, and disaster recovery	Complete system
User Acceptance Test (UAT)	- Confirms the system satisfies business requirements - Initiated after Readiness Certification and system walkthrough - Includes scripts/training provided by Voyatek - Executed by the state personnel and supported by Voyatek	Complete system

End-to-End Application Testing

Voyatek will employ a multi-phase test approach to execute end-to-end testing of the Crossroads system. The test team executes a thorough Testing Plan, each subsequent test phase builds upon the testing foundation initially established during Unit Test to further increase test scope to evaluate functional and non-functional requirements, business processes/transactions, technical behavior, system response and usability.

Integration Test

Integration Test confirms that small, targeted groups of related system components communicate and function correctly (including testing of interfaces). Each system component is tested in each applicable phase including screens, forms, reports, automated processes (batch, real-time, and near real-time), and interfaces. Interface testing occurs in multiple test phases such as Integration, System, and Performance; therefore, it is not a separate test phase.

Voyatek documents the detailed approach and formal Subsystem Integration Test deliverable within the Testing Plan. We will work with the State to plan and scope the Integration Test to

achieve agreed upon requirements coverage and address early testing of core business functions. Testers organize Integration Test functionally and trace test scripts at the component level as related components are developed or configured. We maintain the Requirements Traceability Matrix (RTM) to show the relationship between requirements and test cases/scripts.

Our team creates test cases and detailed test scripts and leverage automation where feasible. We develop modular test cases and detailed test scripts using an iterative approach and proactively seek State and Voyatek peer review. We define scripting standards and guidelines that help our testers maximize test script consistency and reusability. Each test script provides concise, numbered test conditions with clear expected results and test data.

Voyatek prepares realistic Integration Test data and files as necessary and masks any sensitive data derived from Production files, conversion activities, or other sources. We approach test data creation in a holistic, forward-looking manner and design test data and data restore capabilities to serve the current purpose as well as support future system releases and ongoing regression for each software build.

Voyatek executes Integration Test in multiple, logical test cycles for related components, interfaces, subsystems, and applications that implement partial or complete business processes to identify defects and determine System Test readiness. Our team repeats the Unit and Integration Test for defect corrections including appropriate regression testing. Successful tests of core functionality become the basis for ongoing regression testing using an expanding set of reusable scripts and restorable test data.

Voyatek provides thorough documentation of Integration Test results at a summary and detailed level for test script execution results, component coverage, and Integration Test defect information. Thorough Integration testing identifies defects proactively, reduces rework, and builds confidence in the Crossroads System. Integration test scripts and data serve as a foundation that supports subsequent System and Acceptance testing.

System Test

System Test expands upon the scope of Integration Test to validate business processes that functionally and technically span the complete, assembled application. System Test scope addresses the following key considerations:

- End-to-end testing of system-wide business events and use cases
- Valid/exception-based logic and error handling
- Internal and external systems that interact with the Crossroads System
- All new/existing interfaces and batch/automated processing

- System/application-level security, and remote access
- User profiles, privileges, and time-out logic
- Usability testing
- Positive/negative testing to confirm the application functions as expected and does not exhibit undesired behaviors
- Regression testing to confirm subsequent releases do not break previously tested functionality
- We validate the entire assembled system for completeness and accuracy of business processing and system performance.

b) Testing Process

Describe Vendor's process of providing the results of the Vendor's internal testing (unit, integration, performance, end-to-end, life cycle, regression testing, connectivity testing, etc.) A walkthrough of the System to demonstrate that the System is functional and ready for each release UAT will be provided to the State if requested.

- 1. Describe how the Test process will contribute to the thorough quality assurance testing of all software releases, reference database table updates, defect fixes and other Change Requests, are implemented without issue, in accordance with the SLA.*
- 2. Describe how Vendor will provide a written report of release testing results, which the State will review and approve before a release is delivered for UAT.*
- 3. Describe Vendor's process for additional testing that may be required by the State prior to delivery of a release for UAT.*

Voyatek documents the detailed approach and formal System Qualification Test deliverable within the Testing Plan. We work with state to iteratively plan and scope System Test by prioritizing business processes according to transaction criticality, volume, and functional and technical complexity. This prioritization identifies areas for enhanced or in-depth testing that may require additional test scripts, data types/volumes or specific regression testing. Our testers extend the traceability established during Unit and Integration testing to develop and maintain traceability between System Test cases/scripts and requirements.

The test team executes System Test in a dedicated test environment that mimics production as closely as possible in terms of configuration, security, and performance. The System Test environment contains a full data snapshot (rather than partial data sets used in other test phases) that supports parallel functional and technical System and Performance Testing as shown in the figure below.

We conduct review sessions with the state to validate System Test cases/scripts and data collectively address system requirements. As part of System Test, we will evaluate the compatibility of modules across the system and confirm each requirement and system

component is tested in one or more test phases to determine overall system readiness for User Acceptance Test.

Upon completion of System Test entry criteria, the Test team executes System Test in three or more cycles and logs defects and Test script execution results and metrics. We retest System Test defect corrections after testing in lower test environments and perform regression testing as applicable. At the conclusion of System Test, the Test team provides a Readiness Certification of System Test results that details the following testing elements:

- Functional and non-functional requirement coverage/traceability
- Description of overall System Qualification results
- Test script execution results (Passed/Failed)
- System Test defects by functional area, severity, and disposition
- Stability of modules and components in the test environment
- After delivery and acceptance of the Readiness Certification, Voyatek conducts a system walkthrough with the state to demonstrate system readiness for User Acceptance Test.

c) Testing Environment

Describe how the Vendor test environment will be seeded with applicable hardware and data like what will be used for UAT, with all necessary tables populated, etc., so that the System may be fully tested prior to release deployment and as any change requests are developed.

Voyatek will configure, test, and maintain test environments for each test phase to support thorough and efficient testing. [Figure 4](#) below depicts the scope of data included in each environment based on the testing phase(s) that are conducted in each environment.

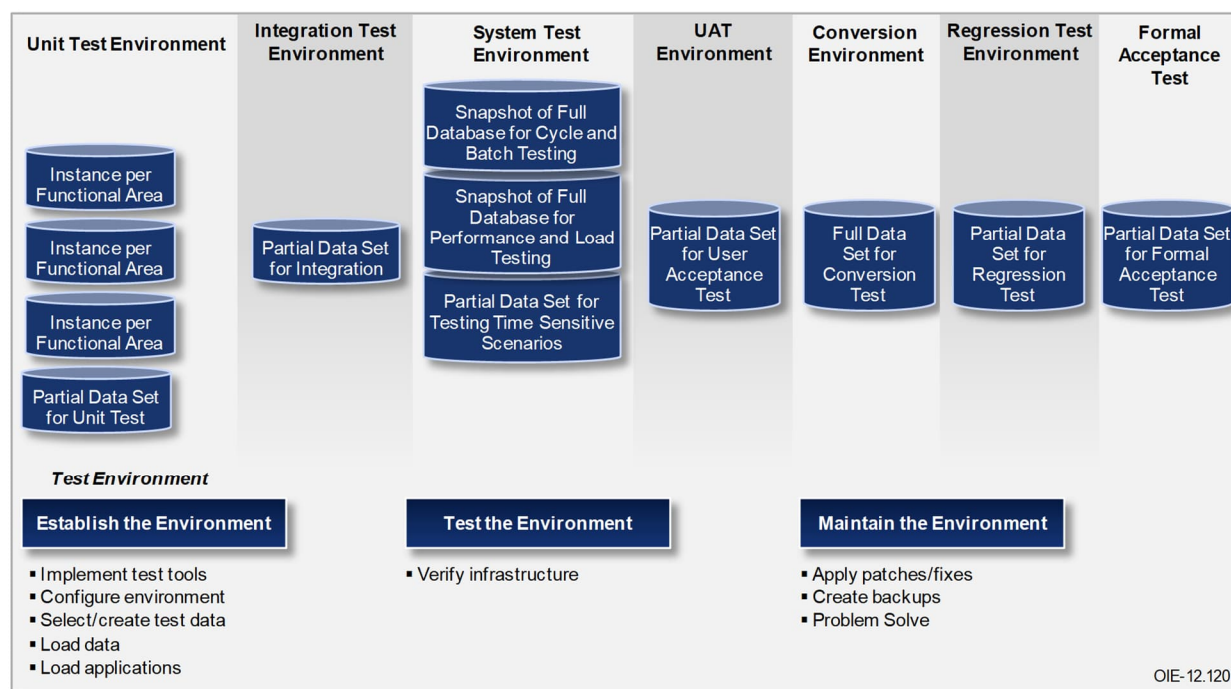


Figure 4: Data Scope by Test Phase / Environment

Voyatek will preload all test data and lookup tables with all data required to successfully execute the test scripts associated with each of the testing phases.

In addition, Voyatek will verify that any hardware that is affected by the release will be thoroughly tested. This includes such hardware as signature pads, scanners, EBT card readers, anthropometric scales, etc.

d) Coordinate with Outside Entities

Describe and explain how the Vendor will coordinate with outside entities (for example, WIC EBT Provider, other third-party interfaces) to ensure that all interfaces and connectivity can be tested.

Over the past 20 years of working with states to modernize and support their WIC systems, Voyatek has developed relationships with vendors that support the WIC mission. It is these relationships that enable Voyatek to implement effectively and efficiently, and work issues associated with third-party interfaces. As shown in the table below Voyatek is currently working with all multiple vendors that support the WIC MIS system.

Table 5: Interface Partners by Type of Interface

Type of Interface	Interface Partner by State
EBT Vendor	Conduent – Georgia, South Carolina, Connecticut, Indiana CDP – Florida, California, Delaware, South Dakota, North Carolina, Solutran – Maryland, Virgin Islands
Secondary Nutrition Education	WIC Heath – Virginia, North Carolina, Florida, South Carolina, Indiana, California, Alabama, JPMA – Rhode Island, Connecticut, West Virginia, Florida,
Signature Pads	Topaz – Florida, Maryland, South Carolina, Georgia, North Carolina ePadLink - Indiana

e) Test Cases / Test Scenarios / Test Scripts and Results

The Vendor will provide test cases / test scenarios / test scripts after contract execution to be used by UAT staff, if requested by the State. Describe in Vendor's proposal the tool and format which Vendor proposes to use to deliver these test artifacts to the State. The test case scenarios will include scenarios that test the System overall, including end of day, end of month, reporting, and disaster recovery activities. The Vendor will work with the State to identify those common scenarios. Test scenarios that need to be re-run due to defects/testing errors will have an identifier in the Test Case Number.

1. The test cases will include the following:

- a. Test Case Number;
- b. Date created;
- c. Author;
- d. Description of Case;
- e. Type of Test;
- f. Required Inputs;
- g. Steps;
- h. Required Set-Up (Preconditions);
- i. Expected Results;

2. Provide Test Results

- a. Actual results;
- b. Run date;
- c. Tester;
- d. Pass / Pass with Exception / Fail;
- e. Failure or Exception reason;
- f. Defects Identified

Voyatek quality assurance staff will develop and maintain a library of test scripts using MS Excel or Word document formats. Tests will include both unscripted and scripted testing of the Crossroads system requirements and will be conducted as new releases of the application are presented as part of the “Release Testing” process.

Voyatek will develop test cases and scripts for the newly developed or modified system functions. Test scripts will be developed to verify that the development matches the requirements and functions according to the Functional Design Documents. Test scripts will take two forms. The first case will be in the form of spread sheets to verify that the system and configuration changes have been incorporated into the system. The second case will be in the form of test cases where requirements and expected results are identified. Both cases will have a column that indicates whether the step/requirement passed or failed.

The following is a sample list of the types of test scripts that will be developed during the project:

- System Changes
- Configuration/Table Changes
- Minor Changes
- EBT Interface, specifically the Food and Nutrition Centers
- Additional changes as identified during the JADs/design validation sessions

The Voyatek testers will set up test scripts detailing the steps that a user might follow to perform the basic functions involved in the certification process. Different scenarios based on “everyday WIC clinic processes,” or threads, will be created as well – allowing for testing diverse ways a user may perform the same task. An example of this would be the use of “Toggling” between participants versus going through multiple screens with the same participant. Voyatek will work with the State and, if present, the QA or IV&V Contractor to identify the common scenarios.

The test cases/scripts will include:

- Test case number
- Date created
- Author
- Description of case
- Type of test
- Input data
- Steps
- Required Set up (preconditions)

Test results will include:

- Expected results
- Actual results
- Pass/fail
- Run date
- Test
- Failure or exception reason

- Defects identified

Testing of any hardware associated with the test script will also be performed, and this testing will be included as part of the test script. This includes such hardware as signature pads, scanners, etc. System processes such as End-of-Day, End-of-Month, reporting and disaster recovery activities will also be tested during this process.

Test Scripts

The following testing subtopics by functional area (topic) will be used for categorizing and grouping testing and issues that may be identified.

Table 6: System Testing Topics for Grouping Tests and Issues

Ref #	Topic / Subtopic
3.1	Certification • Create and Locate Data Records • Manage Application Process • Determine Nutrition Risk of Applicant • Complete Certification • Prescribe Food Package • Process Participant Changes and Transfers
3.2	Nutrition Education, Health Surveillance, and Referrals • Maintain Nutrition Education Data • Perform Participant Referrals • Provide Voter Registration Information • Determine Immunization Status
3.3	Food Management • Maintain Food Categories/Subcategories • Maintain Foods and Food Package Information • Maintain UPC Database and Food Item Maximum Allowed Amounts
3.4	Food Benefit Issuance • Issue Benefits via EBT
3.5	Food Benefit Redemption, Settlement and Reconciliation • Pay Vendor for Food Benefits Redeemed via EBT • Reconcile EBT Benefits
3.6	Financial Management • Manage Grants and Budgets • Monitor Program Expenditures • Process Manufacturer Rebates
3.7	Caseload Management

Ref #	Topic / Subtopic
	• Capture and Maintain Caseload Data • Allocate Caseload • Monitor Caseload
	3.8 Operations Management • Monitor Administrative Operations • Manage Participant Outreach • Monitor Customer Service • Provide Survey Capability • Maintain Inventory • Monitor Program Integrity
	3.9 Vendor Management • Manage Vendor Peer Groups • Create and Locate Data Records • Maintain Vendor Authorizations • Monitor Vendor Training • Support Vendor Communications • Track Routine Monitoring • Coordinate with Food Stamp Program
	3.10 Scheduling • Maintain Master Calendar • Manage Participant Appointments • Generate Appointment Notices
	3.11 Investigations • Create and Locate Data Records • Track Compliance Investigations • Monitor Sanctions and Appeals • Track Confidential High-Risk Vendor Analysis • Track Vendor, Employee and Participant Investigations
	3.12 System Administration • Maintain System Data Tables • Administer System Security • Manage System • Archive System Data
	3.13 Reporting • Generate Standard Reports

f) Virtual Training for the UAT Testing Staff

Describe instructor-led virtual training for the UAT testing staff for topics, if requested by the State and at no additional cost to the State.

Voyatek has been conducting virtual training since the start of COVID. The entire training for the implementation of Georgia's new MIS system was done via virtual training. Over the years, Voyatek has developed methods that enable virtual training to be extremely effective. Depending on the specific training needed, Voyatek will develop either computer-based courses or web-based training via Zoom or Teams. Both methods will include progress validation checks and a final quiz to confirm that the trainees understand the information presented.

g) Describe Onsite Testing Support

Describe a plan for onsite staff to support UAT, if requested by the State.

Should the State request onsite staff to support UAT, Voyatek will send both technical and business staff that are knowledgeable on features being tested. In addition, we will have the business staff pre-run each of the test scripts in the development environment to verify that they are familiar with the data needed to run the test script.

h) Reporting Test or Production Issues

Describe the issue reporting system that the Vendor will provide for UAT testers and State Production users to log issues. The Vendor may also propose to use this issue reporting system as the action item tracking tool. The State currently uses Azure DevOps hosted by the incumbent vendor.

- 1. Describe how the issue reporting system will be hosted by the Vendor, will be browser based and compatible with Microsoft Edge, and not require the licensing or installation of any third-party software on State workstations.*
- 2. Describe how the issue reporting system has the capability to allow users to upload file attachments.*
- 3. Describe the Vendor process to meet WIC confidentiality requirements (7 CFR Part 246.26), such as providing a secure FTP site where sensitive data that cannot be redacted in the issue reporting system can be uploaded by the State to the secure FTP site.*
- 4. Describe how the issue reporting system will have a mechanism for all users to label or tag individual issues in the reporting system with custom labels or tags designed by each user, allowing custom report queries to be executed against the issue database by any user.*
- 5. Describe how the issue reporting system will preserve the date an issue is created, and the date an issue is closed.*
- 6. Describe how the issue reporting system can provide an indicator to distinguish between questions or issues identified by the State in test, identified by the State in production, and identified by the Vendor during their internal efforts.*
- 7. Describe how the Vendor's issue reporting system can be used by the State to log defects that require correction or explanation, requests for additional education and training in functional areas that are working as designed (including any third-party interfaces such as the EBT Provider), and requests for data correction.*

- 8. Describe how the issue reporting system will provide a mechanism for users to create custom queries to identify which issues are in process with the Vendor, and which issues have been returned to the State for retest and closure.*
- 9. Describe how the issue reporting system will have a mechanism for users to subscribe to issue(s) in the reporting system, receiving an email notification of updates to the issues(s).*
- 10. Describe how the Vendor will not close any issues in the issue reporting system without the written permission of the DHHS Release Manager.*
- 11. Describe how, or if, the State may elect to not close an issue until the correction has been monitored by the State and accepted in the production environment.*
- 12. Describe how the Vendor will have a mechanism for mass export of all reported issues and file attachments contained in the issue reporting system, with Vendor performing such mass export upon request of the State.*
- 13. Describe the Vendor's process for granting access credentials to the issue reporting system to third parties upon the request of the State.*
- 14. Describe the Vendor's process for partitioning the issue track system, such that access credentials for each stakeholder can be granted or revoked for each partition.*

During the planning and preparation stage of Integration Testing and System Testing, the test cases, test cycles, and planned test executions will be made available for review. This is not expected to be a formal review but will allow NC WIC resources to review cases before execution. If there are significant issues with the materials, a meeting will be scheduled between NC WIC and Voyatek teams to discuss, and appropriate action will be taken. New materials will be posted to DevOps weekly during the preparation stage. Functional Test cases will be linked to use cases. Use cases will be linked to requirements. Non-Functional Test cases will be linked directly to requirements. In addition, system documentation will be updated as needed to reflect any changes identified by testing.

During the test execution stage, a weekly testing report will be generated and included in the project status report. The test status update will be the responsibility of the Voyatek Test Manager. These reports will be pulled from DevOps and will focus on subject areas such as open defects by severity/ category, and script execution. In addition, a Test Results Report will accompany the end of each testing phase with changes as needed incorporated into the Test Plan.

Voyatek will continue to use Azure DevOps to allow for integrated management of issues, development, system builds, and releases with the following aspects / considerations:

- Attachments can be added to any issue
- Azure DevOps Issue Management is hosted by Voyatek and can be accessed using any web browser.

- Voyatek provides access to a secure FTP site for uploading documents with personal information when necessary.
- Issue Date, Due by Date, and Date Closed are supported.
- Azure DevOps fully supports creation of custom tags. Tags are flexible, allowing for instant lookup or creation of new tags.
- Voyatek user stories differentiate UAT and Production issues during a release epic.
- Tickets can have explanations embedded or tickets can be dragged into a user story for follow up training or review in a WIC status meeting.
- Azure DevOps provides full query support and dashboard creation.
- Issues will not be closed without permission from the Crossroads WIC MIS Release Manager.
- Users can follow issues to receive notification updates.
- Issues can remain in a resolved state that indicate Voyatek work is complete with the status change to “Closed” pending North Carolina action.
- Tickets and queried tickets can be exported as needed.
- Credentials are integrated with SharePoint and managed by Active Directory. Requests for access can be made to the Voyatek product manager. Upon setup, the user will receive an email invitation with their username for initial login.
- During the Kickoff Meeting, Voyatek will review the requirement for partitioning of the Issue Management System. Azure DevOps and SharePoint can support a variety of security configurations. This requirement is not expected to be an issue.

The following is an example of a Dashboard that can be created using the query capability of Azure DevOps.

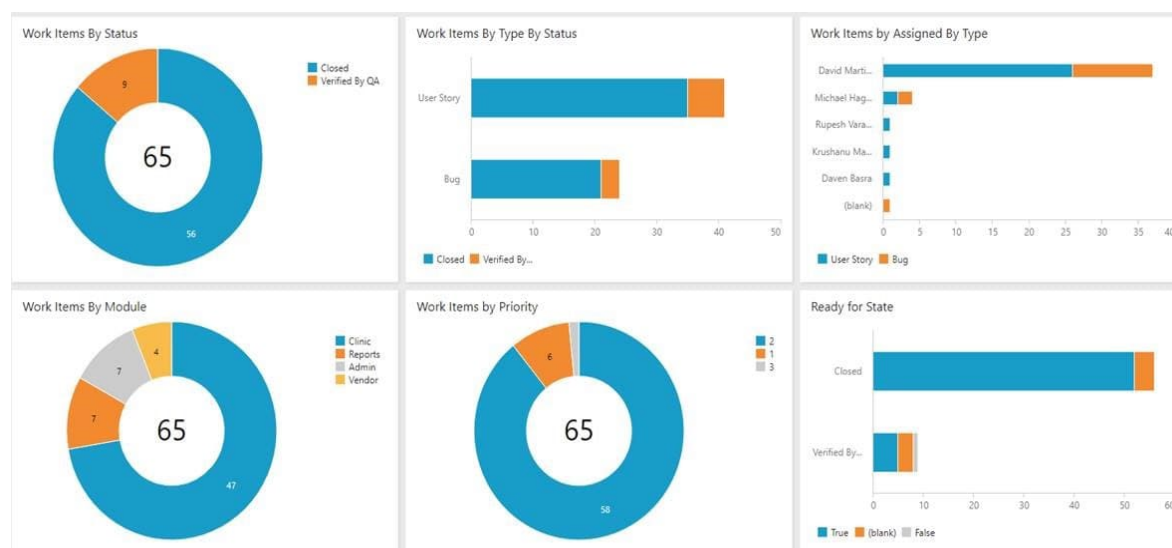


Figure 5: Sample DevOps Project Dashboard

i) Describe the Defect / Issue Fix Process

Describe and explain the process and timeline to fix defects or issues, identified in test or production, in a timely fashion to allow retesting to verify that the identified defects or issues have been corrected. Defects found will be classified by the State using a scale of one (1) to five (5) using a system with similar criteria.

Vendors may propose an alternative Priority / Criteria scheme, that aligns with the issue reporting system

Voyatek acknowledges the defect severity matrix provided by NC WIC and accepts that defect prioritization is at NC WIC discretion within the defect definitions provided. Voyatek will configure Azure DevOps to support the defined defect severity level to allow for the tracking of defects by severity as shown in the following table:

Table 7: Defect / Issue Classification Criteria

Priority Level	Criteria
1	Critical Component Failure: - Does not allow testing to continue - Major malfunction in the System
2	Major Component Failure: - Does not allow testing to continue - Defect or malfunction in certain areas of the System - Problem must be resolved
3	Medium Functional Problem: - Testing can continue - Functions in certain components do not work properly

Priority Level	Criteria
	Components can still work with other components of the System
4	Minor Issue: • Testing can continue • Minor editing error found in a System component
5	Trivial Issue: • Testing can continue • Design Clarification issue • Future enhancement to the System • Cosmetic change needed

j) Time and Cost to Correct Defects

Describe how all defects will be corrected within the time provided in the SLA, at no additional cost to the State. All identified defects will be corrected before the System can be certified as ready for release deployment. Exceptions may be granted by the State if the State determines that there are sufficient alternative processes in place to mitigate the effects of the defect.

1. For reported defects that require software code fixes, describe Vendor's the development and test capacity to correct a minimum of thirty (30) defects per quarter, aggregated from defects reported in both UAT and production.
2. Historically, North Carolina reports approximately sixty (60) non-production and production issues per quarter. These issues include defects that require software code fixes, require non-code fixes to system configuration or system data, or require additional training of State staff.

Voyatek commits to correcting the defects within the time specified in the SLA at no additional cost to the State. Any production defect that the State classifies as severely affecting statewide operations or reporting will be corrected in production by Voyatek within two calendar weeks of the initial report.

Voyatek commits to correcting a minimum of 30 defects and 60 issues per quarter. Having supported the NC Crossroads system for the past six years, we are keenly aware of the number of code fixes and issues that are encountered on a weekly, monthly, and quarterly basis. We will provide sufficient staff to make sure that the NC Crossroads system continues to support both the clinic and state staff effectively and as designed.

k) UAT Completion Report

Describe the Vendor's comprehensive checklist of items that will be included in each UAT Completion Report, to demonstrate the successful completion of each release UAT and the readiness of the System to move to deployment. The Vendor will provide a formal presentation to the State if requested, including a written certification report that the System is ready to proceed to deployment.

At the completion of each UAT, the Voyatek Test Manager will prepare a UAT Completion Report that describes the activities and results of each UAT and the readiness of the Crossroads system release to be deployed to Production. Voyatek will include the following topics in the report:

- Type of testing performed
- Test database generation
- Test case development, evidence and schedule
- Modifications included in the release
- UAT Completion Checklist status:
 - o Connectivity to the Production System is ready
 - o User Documentation is ready
 - o Real time connectivity to the EBT Vendor's production site is ready
 - o Backup system is ready
 - o Training activities and materials are ready
 - o Help desk and hardware support is ready
 - o Data migration for pilot sites is ready
 - o Test and Development system will be loaded with a copy of Production (to support issue resolution)
 - o Issue/Bug status has been updated
- Voyatek Recommendation

If requested by the State, Voyatek will provide a formal presentation of UAT completion and readiness for production, including a written certification that the Crossroads system is ready to proceed to Production deployment.

I) IV&V / QA

The State or FNS may utilize outside Vendors to perform third-party Quality Assurance or Independent Verification and Validation activities throughout the course of this contract. The Crossroads Vendor will be responsible for coordinating / cooperating with these QA / IV&V Vendors.

Describe Vendor's experiences in working with IV&V / QA Contractors on WIC MIS, WIC EBT, or other similar projects.

Voyatek has experience working with external IV&V and quality assurance contracts during various implementation and maintenance projects over the past two decades. We have had the opportunity to work with most of the major IV&V contractors working within the WIC marketplace. In addition, Voyatek has a history of successful WIC MIS implementations and maintenance contracts that were completed within cost and schedule requirements. Part of that success has been the ability to work well with third parties including IV&V, quality assurance, and EBT contractors. If North Carolina engages an IV&V or QA vendor, the Voyatek product manager

and project team will work that contractor's staff as a part of the overall NC team. We understand the important contributions these entities provide in ensuring successful WIC projects.

m) Data Correction

Describe the Vendor's approach to perform test or production data correction, upon request of the State and with written permission from the State, as needed for data issues where it is not possible or practical for the State to correct, such as correcting corrupted/non-editable fields, correcting inaccurate data caused by software problems, etc.

- 1. Describe how this data correction, for issues both due to actions of the State and actions of the Vendor, can be performed by the Vendor at no additional cost to the State.*
- 2. Describe how results of testing of the data correction will be provided to the State upon request and accepted by the State prior to execution of the data correction in a production environment.*

When requested by the State, the Voyatek team will perform test or production data correction at no additional cost. Our experienced team can provide this service with speed and efficiency due to their deep understanding of the Crossroads data model and functionality. Following data correction, we will test the related system functionality to confirm that the corrected data is interacting with the system correctly.

In some cases, it may be best to test the data correction in a test environment first. If desired by the State, the testing results will be provided to the State for approval prior to correction of the equivalent data in the production environment.

Voyatek will track data correction requests in a Data Correction Log so that the history of data correction not made via the system is available as needed. The log will include data elements such as:

- Request Number
- Request Date
- Requested by
- Approved By
- Requested Change Description
- Reason for the Change
- Implemented Change (SQL Script)
- Change/Test Data (Data output or number of records updated)
- Comments

In addition, Voyatek will continue to update the Help Desk Module, which was first developed for WoW states and then adapted for use in Crossroads. The module allows state help desk staff to address several common support issues that previously required M&E vendor support such as changing a participant's gender or date of birth. The module creates an audited interface that

performs updates and automatically checks for potential impacts like changing a participant's certification status because of an age change. The Help Desk Module improves the speed and reliability of common help desk corrections and allows for more effective use of state staff time.

3.5.9 Installation Support for New Builds

Describe Vendor's approach to provide installation support, as listed below, for the Crossroads system for a maximum of six (6) Vendor-managed cloud environments, such as UAT, various secondary testing, production, etc. These environments will be determined by the State and be itemized in a matrix to be maintained by the Vendor.

a. Describe how the Vendor will coordinate scheduling and installation procedures with technical staff in North Carolina and how the Vendor will request and maintain access credentials to applicable servers that have been granted to the Vendor.

b. Describe how the Vendor will upload the Crossroads system to the appropriate cloud server(s) to support a statewide deployment and will perform necessary backups of the application and databases as a contingency.

c. Describe how the Vendor will unpack and install the products into the rehosted servers (web application server, database server, report server, and batch server) as required for the cloud deployment, including how Vendor will execute all necessary database scripts. And how Vendor will not embed or execute any script against an environment's database without prior written approval from the State.

d. Describe how the Vendor will stop and start Crossroads services as required during the deployment, including the Vendor coordinating with State staff depending on access privileges granted to the Vendor.

e. Describe how the Vendor will maintain a deployment checklist to capture lessons learned, to be shared with State staff.

f. Describe how the Vendor will perform an initial "smoke test" of the Crossroads system, including the batch and report cloud servers, prior to informing the State that the deployment is complete. Describe how the Vendor will obtain prior written approval from the State regarding restoring the backups of the application and databases should there be a critical system failure identified during smoke testing.

g. Describe how the Vendor will provide for each build via secure FTP:

- 1. An ISO image of the complete, cumulative source code, including instructions and prerequisites required to compile and produce executable code;*
- 2. A ZIP file (compatible with the pkware standard) of the executable code and installation scripts used by the Vendor during the install, database scripts applicable to the database server, and reports for the report server that was implemented. Describe the process for how this code and scripts can be utilized on any of the supported State environments.*

h. Describe how the Vendor will provide release notes and a refreshed environment summary matrix showing the level of Crossroads installed in each environment. Describe how the release notes will contain at a minimum:

- 1. The Build Number.*
- 2. A detailed description of new Change Requests delivered in the build.*
- 3. A detailed description of any new Reports delivered in the build.*

- 4. A complete description of all defect corrections, including the defect reporting number(s), delivered in the build. This list will be separated by defects reported in Production, defects reported in Test, defects identified by the Vendor, and any permanent fix of any hotfixes previously applied to an environment.*
- 5. A complete list and description of any system tables added, changed or removed.*
- 6. A detailed description, including illustrations of affected system screens, of any corrective, adaptive, or perfective changes made by the Vendor to address issues found during QA efforts.*
- 7. All details needed for the State to accurately update automated performance testing scripts and other tools.*
- 8. Comments and additional information; and*
- 9. The audience for Release Notes is both State WIC staff and State IT. Notes will be written using non-technical IT language that can be understood by State WIC staff.*
- i. Describe how the Vendor will email State staff at the start, as needed during installation, and at completion of each deployment.*
- j. Describe how the The Environment Summary Matrix will be updated, listing the applicable defect reporting number(s), and provided to the State after any hotfix is applied to an environment.*
- k. Describe how the Vendor will provide and maintain a complete installation and configuration guide, detailing how to perform fresh ground-up installs of the system on cloud servers and workstations.*
- l. Describe in detail on how production installation services will be performed after Business hours, including all State, Federal, and Vendor holidays and weekends, as requested by the State. Production upgrades typically begin on Saturdays between 8:00 AM and 6:00 PM Eastern Time to minimize disruption to the NC local agencies, with day and time subject to change at the discretion of the State.*

During Transition-In, with the rehosting of NC Crossroads to Azure, the Voyatek team will assume responsibility for platform operations and will have proper credentials to manage the NC Crossroads system environments. Coordination with NC DIT for platform maintenance and operations will no longer be necessary.

A key part of Voyatek's work in North Carolina over the past several years was to automate the system build and deployment processes. Azure DevOps was configured with pipelines that handled the build process from start to end, including publishing defined output artifacts. These artifacts are then consumed by Octopus Deploy, which deploys the system to environments in the state, including staging, sandbox, training, UAT, and production. There are approximately 75 steps involved in a deployment, which are scripted and managed in Octopus Deploy. A full release takes about 30 minutes from the start of the build in Azure DevOps to a deployment to the initial environment. Subsequent deployments to internal and customer environments take about 15 minutes and can be done at any time. This automation handles processes such as stopping and starting services, transferring files, unpacking components, etc.

Deployment automation starts in Azure DevOps, which stores source code and manages the build process. Automating deployment includes the following steps:

- Retrieving source code from a code branch based on the targeted release version
- Compiling the code into executable form
- Running unit tests
- Linking code changes in the release to work items such as user stories and bugs
- Creating deployment packages from compiled code that are published to environments
- Publishing build results and linked work items
- Creating release notes

Once the code is built, Voyatek utilizes the Octopus Deploy platform for deploying Crossroads code to environments. **Octopus uses the same process for all the environments, which keeps them consistent with one another and makes environment management and troubleshooting much easier.** Octopus stores environment configuration settings separately from the deployment process. Each environment has its own settings for database connection strings, file locations, and other configurable system data. Where there are minor differences in environments, the deployment path can be branched to accommodate these.

We also require progressive deployment of code to hosting environments. For example, code cannot be deployed to production without first being deployed to lower test and UAT environments. This prevents code differences between environments while ensuring that code is tested before being promoted to higher environments.

Database deployments, such as schema changes and data updates, are also handled by Octopus. Developers write changes to scripts separately and in a defined order. Octopus then applies these changes in the target environment. A list of what scripts have been run in each database is used to determine which ones need to be executed as part of a deployment. This allows the process to work against any environment, bringing it up to date, regardless of whether deployments have been made recently or not. The figure below shows a typical release pipeline graphic in our automated deployment software.

The screenshot shows the 'Crossroads Overview' dashboard. It features a navigation menu on the left with options like 'Dashboard', 'Projects', 'Infrastructure', 'Tenants', 'Insights', 'Library', and 'Tasks'. The main content area displays a table of releases. The table has columns for 'Tenant', 'Development', 'Test', 'Sandbox', 'Training', and 'UAT'. The 'Development' column shows a release for 'Alabama' with a status of 'Pending Approval' (indicated by a red 'X' icon). The 'Test' column shows a release for 'Internal' with a status of 'Approved' (indicated by a green checkmark icon). The 'UAT' column shows a release for 'Rhode Island' with a status of 'Approved' (indicated by a green checkmark icon). The table also includes a 'Filter by release' dropdown and a 'Group by' dropdown. A 'CREATE RELEASE' button is visible in the top left corner of the dashboard.

Tenant	Development	Test	Sandbox	Training	UAT
Alabama	Pending Approval	Approved	Pending Approval	Pending Approval	Pending Approval
Internal	Approved	Pending Approval	Pending Approval	Pending Approval	Pending Approval
Rhode Island	Pending Approval	Approved	Pending Approval	Pending Approval	Approved

Figure 6: Release Pipeline with Pending Approval for Customer Environment Deployment

Once updates are approved for deployment, the automated processes work together to publish them to the hosting environment quickly and reliably, eliminating human error and applying security guidelines consistently. Our automated deployment approach has reduced the need for extensive UAT testing of system infrastructure and makes system upgrades as seamless as possible. This reliability has led many customers to move to more agile release processes with a faster release cadence, which helps states respond quickly to FNS policy changes.

Voyatek has successfully implemented deployment automation with Crossroads states including North Carolina (on-premises), Rhode Island (Azure Cloud), and Crossroads User Group development and test environments (Azure Cloud). This is a critical component in our ability to deliver high quality releases on time. As North Carolina Crossroads is rehosted to Azure, the same build and deployment processes will be used.

Voyatek will coordinate with the NC Crossroads WIC MIS Release Manager on the schedule and contents of each Crossroads release and will provide notification of each scheduled release of Crossroads along with detailed release notes. Production releases will only be performed when approved by the Release Manager, typically on weekends or holidays when clinics are closed.

3.5.10 Deployment of Releases for Statewide Production

Describe Vendor's approach to providing the following services and tasks under this category.

a) Complete Migration

The Awarded Vendor will complete migration from the State-hosted production environment to the Vendor-managed cloud production environment before the end of the Transition-In Phase. This includes migration of all applications (WPF and portals), databases, and file system contents.

During the Transition-In phase, the Voyatek team will complete the rehosting (migration) of Crossroads from the NC Data Center to our Nutrition Azure cloud. [Appendix E: Rehosting Implementation and Rollout Plan](#) contains the details of how this migration will be planned, communicated, executed, and validated. The migration will include all of the NC Crossroads system including the associated portals.

b) Detailed Production Deployment Plan

How Vendor will provide a detailed Production Deployment Plan after contract execution that describes the procedures, detailed schedules, and resources needed to implement and immediately support each release of Crossroads statewide. The Plan will be submitted as stipulated in Table 1 – List of Product Deliverables.

A minimum of two hundred (200) hours of Change Requests and a minimum of twenty (20) defect corrections (or smaller minimums at the sole discretion of the State), will be developed, tested, and delivered for UAT along with its final UAT Readiness Report no later than ninety (90) Calendar Days from the start of the Maintenance and Enhancement Phase.

Following contract execution, during Transition-In and at least 90 calendar days prior to the first Statewide deployment in the new Azure environment, Voyatek will publish the Production Deployment Plan, which will include the following:

- Development, testing, UAT, and deployment schedule
- Resource plan for a minimum of 200 hours of change orders and 20 defect corrections (or less as determined by NC WIC) to be included in the first release to Azure
- Procedures for development, testing, documentation, and UAT support
- Description of any database modifications necessary for the content of the release
- Description of coordination required with outside entities including the EBT Contractor as needed based on modifications in the release scope
- Description of the process of UAT testing and system demonstration necessary to determine readiness for production use
- Process for developing and coordinating the production release schedule
- Schedule and process for updating system documentation including:
 - o Detailed Functional Design Documents (DFDD), including a detailed Risk Code Summary Matrix and Trigger Summary
 - o User Manuals
 - o Detailed Technical Specifications (DTS)
 - o Data Dictionary
 - o Interface Control Documents (ICD)
 - o External Communication Documentation (ECD)
 - o Report Definition Documentation (RDD)
 - o Installation and Configuration Instructions

- o Central Processing Site Operations Manual
- o White Papers as needed
- Processes to monitor system housekeeping functions
- Verification that WIC EBT Processes are operating successfully and corrective action in the event of a failure
- Help Desk support for state staff
- Development of guidance documentation for system functions
- Error logging procedures
- Process and timeline to fix system errors identified within the release
- Procedures for rollback in case of a system failure

The Production Deployment Plan will be delivered to the State for review and comment prior to being finalized for execution.

c) UAT Results

Describe how the results of UAT and a walkthrough of the System will demonstrate that the System is functional and ready for statewide deployment in a production environment.

Voyatek will work with NC WIC to determine the extent of the UAT the State wishes to conduct for the transition to Azure and the scope of changes in the first release. Prior to the UAT, Voyatek will conduct a walkthrough of the system working in the cloud environment and the enhancements contained in the first cloud release.

d) Seeding the Production Environment

Describe how the production environment will be seeded with necessary data that will be used for statewide deployment and populating all necessary tables, etc., so that the System may be fully operational as sites encounter the new release in production.

The Azure cloud environment databases will be a migration of the on-premises databases running in the NC Data Center. The only seeding of data that will be necessary is for new tables or columns that are added to support enhancements in the first Azure release. This is the same procedure that Voyatek follows for any release with new database tables or columns.

e) Coordination with Outside Entities

Describe and explain how the Vendor will coordinate with outside entities (WIC EBT Provider, etc.) to ensure that all interfaces and connectivity will be operational.

With each release, Voyatek will coordinate testing and release to production activity with interface partners impacted by changes to the functionality of the Crossroads interfaces in that release. For releases that do not impact the functionality of any given interface, Voyatek will verify that the interfaces are working correctly via normal system monitoring.

f) Deployment Schedule

Describe how the Vendor will participate with State staff to determine the deployment schedule.

Voyatek will work with the Crossroads WIC MIS Release Manager and key WIC staff to determine the functionality (defect repairs and enhancements) that will be included in each release of Crossroads and the planned deployment schedule for each release. With the automated deployment process we have implemented, North Carolina is now able to implement smaller releases more often to provide improved reliability and fewer changes for WIC staff to consume with each release.

g) System Documentation Updates

Describe how the Vendor will provide to the State updates to the following System documentation in a timely manner prior to deployment of each major system release to reflect all software Change Requests and defect corrections:

- 1. Detailed Functional Design Documents (DFDD), including a detailed Risk Code Summary Matrix and Trigger Summary;*
- 2. User Manuals;*
- 3. Detailed Technical Specifications (DTS), including Data Dictionary (currently available in Compiled HTML (CHM) format) and a detailed listing of all System Tables;*
- 4. Interface Control Document (ICD) for the WIC Universal MIS-EBT Interface (WUMEI);*
- 5. External Communication Documentation (ECD);*
- 6. Report Definition Documentation (RDD);*
- 7. Installation and Configuration Instructions, including hardware and software prerequisites;*
- 8. Central Processing Site Operations Manual;*
- 9. White Papers to provide written guidance to assist the State with understanding or solving an issue.*
- 10. The above System documentation will be maintained in Microsoft Office 365 format, that is editable by State staff, and provide all ancillary files used for the creation of embedded figures, diagrams, tables, or other non-editable components of the documentation.*

Voyatek maintains system documentation, training manuals, quick reference guides, detailed specifications, and Captivate training materials for our WIC customers. Throughout the contract, Voyatek will maintain the system documentation accurately and completely. We will utilize SharePoint as the document repository and for managing version control for system documents and deliverables. With each release, we will update the system documentation appropriately, deliver it in both draft and final versions, and provide it as part of the final release package along with a copy of the updated source code. The details of maintenance for each element of Crossroads system documentation will be included in the Production Deployment Plan.

h) Business Rules Development

Describe how the Vendor will assist, at no additional cost, with the development of business rules and other guidance with North Carolina WIC to govern program operations.

For the development of change requests (and occasional clarification of business logic for defects), the Voyatek Business Analyst Manager will work with the NC WIC staff to develop the requirements and associated business rules as a part of the change request design process. These business rules will be captured as a part of the documentation of the change request.

Our team's deep understanding of the original Crossroads design intent and reasoning will continuously provide value to the NC WIC staff in determining the best approach to implementing system enhancements that integrate well with the whole system design. This participation in system design changes is vital to our M&E work and will be provided to North Carolina at no additional cost.

i) Statewide Deployment Release Support

Detail how the Vendor will support statewide deployment of release including the following:

- 1. Monitoring end of day processing to ensure successful completion by the start of the next Business Day, taking corrective action as needed, and reporting the status to North Carolina WIC.*
- 2. Verifying that System housekeeping functions have been completed, taking corrective action as needed, and reporting the status to North Carolina WIC.*
- 3. Verifying that appropriate files have been sent to / received from the WIC EBT Provider and others, processed, taking corrective action as needed, and reporting the status to North Carolina WIC.*
- 4. Providing Help Desk support to State Office staff.*

With the transition of Crossroads hosting to Azure, Voyatek will assume operational support for the Crossroads system. This includes monitoring end-of-day processing, normal housekeeping functions, verifying interface interactions, and all other aspects of platform monitoring and maintenance. These activities will be a part of everyday system monitoring.

For a description of our Help Desk support for State Office staff, see [3.5.7 Help Desk Services](#).

j) Error Logging System

Describe and detail the error logging system that the Vendor will provide or monitor for implemented sites to log errors.

Crossroads has built-in error logging which is reviewed regularly by the Voyatek technical team. Errors are reviewed for possible system code issues that need to be corrected or perhaps minor design adjustments to prevent an error such as a data-driven issue from occurring. System

defects will be logged for correction and potential design improvements will be presented to NC WIC for consideration.

k) Process and Timeline to Fix All Errors

Describe and explain the process and timeline to fix all errors in a timely fashion to allow rapid retesting to verify that the errors have been corrected. Describe how all Critical Component Failure and Major Component Failure severity errors will be corrected within the time provided in the SLA. Describe how all identified defects will be corrected before the System can be certified as ready for Statewide Deployment. Exceptions may be granted if the State determines that there are sufficient alternative processes in place to mitigate the effects of the defect.

Errors that are caught by the Voyatek test team during integration or system testing are logged and corrected prior to UAT. Errors identified during UAT or in Production will be reviewed with the State staff and the NC Crossroads WIC MIS Release Manager to determine the best approach for correction of these errors based on their severity. Critical Component Failures or Major Component Failures will be addressed promptly and fixed within the time detailed in the SLA. If the error is in Production, a corrective release will be planned. Less severe errors may be determined to be best corrected in a subsequent release. NC WIC will make this determination.

l) Deployment Plan

Describe how the Vendor will provide in the Deployment Plan the procedures for application and database rollback in the event of a significant release failure in the production environment. Describe the procedures for preserving new production data that would otherwise be lost following a database rollback.

The Production Deployment Plan will include procedures for application rollback should a release encounter a significant failure such that rollback is the best option. In Voyatek's experience, this is an extremely rare event. However, should it occur, the application rollback to the prior release is quick and easy due to our automated deployment strategy.

Database rollback would only be necessary if the release in question contained database structural changes that were not supported by the prior release or if certain data elements contained new values that were not available in the prior release. In such a case, the Voyatek team will make a copy of the database prior to application rollback and perform the detailed analysis to determine which records were inserted or updated after the problem release was deployed to Production. The data management strategy will depend on the circumstances. The Voyatek lead personnel will work with the NC WIC staff to verify that data is not lost, and all data integrity is maintained with the rollback.

3.5.11 System Training

Describe Vendor's approach for training all State staff that will participate in a release UAT onsite in North Carolina, if requested by the State.

Through a proven, structured training approach, Voyatek will provide training for State staff that will participate in the UAT of any upcoming release as needed. The level of training will depend on the scope of the changes in the release and the complexity of the enhancements being deployed. Often webinar training will be sufficient, which is quick and convenient for busy State staff. However, for more complex new features and functionality, formal classroom hands-on training may be appropriate. Upon request by the State, Voyatek will provide on-site training to the State UAT test team.

Our approach includes building real-world examples that will be seen in clinics. This approach will be tailored to meet the State's needs by working closely with the State's WIC senior staff to verify that course instruction for system trainers, end users, and technical support personnel is complete, easily understood and meets as many real-world situations as possible. The development of each of the training activities entails the following steps:

- Curriculum Design
- Training Development
- Training Implementation

The training will consist of a thorough overview of the functional processes of the system, with emphasis on new functionalities. Training scenarios will be provided for each function to be performed. Each scenario will be built upon one another as more system functions are thoroughly explained. Voyatek will work with the State to verify that appropriate scenarios are included in each type of training.

During UAT, Voyatek staff will support the State UAT Test Team with any technical assistance. For assistance with how to perform a functionality associated with a test script, team members will be directed to use the provided user training materials and online help. Having the test team consult the user training materials while conducting UAT will identify any deficiencies in the training materials. Any such deficiencies will be corrected prior to final acceptance of the training materials by the State.

3.5.12 Change Request Process

Describe Vendor's approach for completing System enhancements and modifications to improve the operation or functionality of the System, to comply with new Federal regulations or requirements, to comply with changes in State policy and procedure, or to meet other corrective, adaptive, or perfective needs via work authorization / supplemental hours. This process applies only to enhancements and modifications to the Crossroads system.

a) Adhering to the Prescribed Change Request process

The following services and tasks are required under this category at no additional cost to the State. These specifications do not constitute or imply any promise or intention for the State to fund or approve Change Requests. Adhering to the prescribed Change Request process as follows:

1. Explain how the Vendor can review the CR Concept, ask for clarifications when needed, identify associated risks with the CR Concept when appropriate and then prepare a CR Response fifteen (15) Calendar Days of receipt of the CR Concept for State review and approval within. The CR Response will include the Vendor's understanding of the original CR Concept with high-level detail like content provided in the original CR Concept, and a high-level non-binding system design outlining what Crossroads functions and screens are affected and conceptual estimate of hours and cost.
2. Explain how the State can review, modify and approve the CR Response as appropriate and notify the Vendor. The Vendor will then prepare a detailed system design document and binding hour and cost estimates (CR Draft Estimate) within fifteen (15) Calendar Days of receipt of the State approval of the CR Response, or within thirty (30) Calendar Days of the State's approval of a CR Response which the Vendor estimates will require three hundred (300) hours or more to complete (Major CR).
3. Explain how the State can review the CR Draft Estimate and notify the Vendor within thirty (30) Calendar Days, or longer if USDA/FNS approval of the CR Draft Estimate is required, that is approved, requires further rework, put on hold, or withdrawn. Approved CR Draft Estimates will be signed by the State and returned to the Vendor. The Vendor will then sign and return the CR Draft Estimate to the State
4. Explain how the Vendor can offer and coordinate cost sharing of common code changes among any other WIC States where the Vendor maintains and enhances any version of Crossroads or similar functionality that can be used across the Vendor's MIS offerings.
5. Explain how the Vendor can obtain mutual agreement with the State on a deployment schedule for approved CR Estimates that considers the urgency of the change and the need to meet Federal deployment deadlines as appropriate.
 - i. Explain how approved changes requiring less than three hundred (300) hours can be developed, tested and delivered for UAT within sixty (60) Calendar Days of State approval of the CR Draft Estimate, and how approved changes requiring three hundred (300) hours or more can be developed, tested and delivered for UAT within ninety (90) Calendar Days of State approval of the CR Draft Estimate.
 - ii. Explain how the Vendor has the staff, equipment, and all other resources to develop and test approximately one hundred fifty (150) hours of approved Change Requests per quarter, if requested by the State. Explain how the Vendor will address situations where more hours are required.

Voyatek acknowledges the System Change Request (CR) Process as described in the RFP. The table shown below summarizes our understanding of the process with roles and responsibilities to clearly demonstrate how the process works between our team and the NC WIC team.

Table 8: Change Request Process – Roles and Responsibilities

Process Step	State Role	Voyatek Role	Task(s)	Timeframe
1. CR Initiation	Initiate Request	Log & Track Request	Provide CR Concept to Voyatek	N/A
2. CR Validation	Provide Clarifications	Validate CR	Verify minimum information required to proceed	N/A

Process Step	State Role	Voyatek Role	Task(s)	Timeframe
3. Provide Initial CR Response	State Review/Approve Initial CR Response	Prepare Initial CR Response	Identify functions impacted and potential risks. High level design, and Estimated hours and Costs.	Within 15 calendar days
4. Authorize and Prepare Detailed Analysis and CR Draft Estimate	Review, Modify and Approve Initial CR Response	Prepare Detailed Response & CR Draft Estimate	Detailed System Design document, and binding hour and cost estimates (CR Draft Estimate)	Less than 300 hr. – within 15 calendar days, otherwise 30 calendar days
5. CR Authorization	Review, Approve or Hold CR	Track/ Execute CR	Execute changes, and prepare for deployment	Within 30 calendar days, longer if FNS approval is needed
6. CR Deployment	Discuss CR deployment with Voyatek	Mutually agree on a Deployment Schedule	Schedule CR Release as requested	Less than 300 hr. within 60 calendar days, otherwise 90 calendar days

Voyatek strives to maintain the integrity of the production environment through planning, scheduling, and successfully deploying system changes packaged as releases. Release management is tightly coupled with the change management process. The change management process schedules and approves each individual change. Release management then combines these approved changes into logical packages (both process-related and technology-related changes), reducing the frequency of changes to Production and minimizing business disruption. Change management then authorizes the release. Voyatek is proposing three types of releases as described below.

Development (Major) Release: Changes that have a major impact to the Crossroads system and require significant time to develop, test and implement. As requested in the RFP, Voyatek is planning to deploy three major releases per year, one every approximately 120 calendar days. Change requests requiring over 300 hours would probably fit best in one of these releases, unless otherwise required by NC WIC.

Maintenance Release: Standard changes placed into scheduled service packs; for example, bi-monthly maintenance release. Change requests requiring less than 300 hours of effort would likely be included in one of these releases.

Emergency Release: Changes needed to be moved into production quickly to address a significant issue. These are done on short notice (5 calendar days) when a critical change is identified as part issue management.

Voyatek's Release Management Process actively manages the change deployment process including version control, access to testing facilities, batching of changes, oversight of system changes, post-implementation validation, and production documentation updates. The process addresses all aspects of the release implementation, including tasks performed outside of the system to prepare for the implementation. Examples of items considered are:

- **Release Date** – First and foremost, the actual implementation date must be established and agreed to.
- **Deployment Items/Activities/Schedule** (including preparatory programs) – This includes activities, tasks, and owners.
- **Readiness Checklist** – Establish the tasks that must be completed prior to the release date. The following is a sample, and the contents of this checklist will vary based on the type and contents of each release:
 - All milestones and deliverables on the schedule completed
 - Data preparation activities completed
 - External interface partner work completed (as applicable, for example, EBT Provider export modifications on their system)
 - Release notes and communications prepared for release
 - System documentation updated
 - Training completed
 - Configuration audits passed
 - Hardware environment in place, upgraded, etc.
 - All quality assurance issues resolved or addressed
 - Operational procedures updated and communicated

Voyatek acknowledges that when preexisting solutions have been developed using federal funds and which are transferable from other agencies, if requested by NC WIC, Voyatek will transfer those solutions. The transfer of existing solutions will be performed per the change control process, but estimated costs will reflect only the cost to transfer the preexisting solution. Voyatek utilizes this process extensively to support many WIC programs in a cost-effective manner. Examples of this work range from the transfer of entire modules, like the Peer Counseling module, to the transfer of simple scripts to do things like load income eligibility updates.

Voyatek is also an active partner in addressing evolving FNS policies and WIC program needs. One advantage of working with Voyatek is our ability to respond efficiently to changing FNS policies and evolving challenges to the WIC community based on the breadth of our WIC customer base. For example, when new policy updates are published, we create a work group consisting of team subject matter experts with state agency experience, technical and project leads to review policy guidance and design proposed solutions that meet new policy requirements. We include alternative solutions to meet WIC program expectations and differences to share with State WIC staff. The goal is to develop reusable and easily transferable updates and procedures that allow states to implement changes quickly and efficiently. This approach has allowed Voyatek states to respond quickly to many changes such as Cash Value Benefits policy, Covid related waivers, and the formula shortage. The project team will be prepared to provide proactive analysis and options to NC WIC as well as to gather requirements specific to NC WIC.

Voyatek has proposed a team and organization that is prepared to meet the required levels of system changes anticipated and requested by North Carolina (approximately 150 hours of approved change requests per quarter) as we have demonstrated throughout the current contract. Voyatek has a significant depth of technical resources in our WIC Practice with over 80 team members who are familiar with WIC programs and requirements. If the proposed NC support team requires additional resources to meet the demand for system change requests, the Voyatek product manager will work with the executive oversight team to redirect company resources as needed to meet North Carolina objectives.

b) Changes to Reference Tables

Changes to reference tables are not billable changes but are normal system maintenance activities covered at no additional cost. Reference table changes will still be initiated by a CR from the State and a corresponding CR Response from the Vendor but will not require the detailed system design document unless the CR affects existing System Documentation.

The Vendor will be responsible for making all reference table changes within five (5) Calendar Days of State approval of the CR Response.

Activities that can typically be completed independent of a Production release such as (e.g., data set expansions, data purges) are completed on a more frequent basis (e.g., daily or weekly) as agreed with the State. This type of activity includes changes to reference tables which will be initiated by a CR from the State and a corresponding CR Response from Voyatek. Reference table changes will not require updates to the system design documentation unless the CR itself affects existing system documentation. All reference table changes will be completed within five calendar days of State approval of the CR Response and at no additional cost to the State.

c) Out-of-Scope Changes

Changes to the System that are outside of the scope of this RFP, the Vendor's proposal, and the existing Crossroads Detailed Functional Design Documentation will be considered for additional cost and will go through the full change request process described above.

In accordance with the RFP, changes to the system that are outside of the scope described in this RFP, Voyatek's proposal, and the existing Crossroads Detailed Functional Design Document will be considered for additional cost and will go through the full change request process described above.

d) EBT Interface Changes

Changes to the EBT interface, including FMNP, will be implemented by the Vendor at no additional cost to the State. Such changes will be initiated by a CR Concept from the State and a corresponding CR Response and CR Draft Estimate from the Vendor, provided however that such CR Draft Estimate will be at no cost to the State.

As per the RFP, changes to the EBT interface, including FMNP, will be implemented at no additional cost to the State. Such changes will be initiated by a CR Concept from the State and a corresponding CR Response and CR Draft Estimate will be provided by Voyatek. We acknowledge that such a CR Draft Estimate will be at no cost to the State.

e) Example of Change Requests

Describe at least three (3) change request items, from the Vendor's experience, that the Vendor has implemented. Describe creative opportunities and best practices that will minimize or mitigate change requests and potential costs associated with change requests, such as cost sharing with other State WIC Programs that may be contracted with the Vendor.

Voyatek is continually working with our existing customers in enhancing their MIS system to make the administration of the WIC system more effective and efficient. **As system upgrades and changes are made to other systems, Voyatek can provide these same enhancements to North Carolina expediently and without risk.** We have transferred many such functions (report visualizations, participation dashboard, nutrition education, UPC submission, formula exchange function, NTE functionality, portals, etc.) between other states' systems. Voyatek also developed the new USDA Food Delivery Portal (FDP) for South Carolina and has shared the research with other system project teams.

The following are several examples of change requests that have been completed in the last year:

- North Carolina eFMNP – This enhancement implemented EBT for Farmer's Market (FM) with the state's existing EBT vendor. The solution allows for Crossroads families to have both a Farmer's Market EBT card and an eWIC EBT card to maintain segregation of FM and WIC data from issuance through redemption.

- North Carolina Automated Benefit Issuance – This change, currently in UAT, will provide clinics with the ability to preview participants who are eligible for their next set of benefits. Multiple search filters help staff to prepare participant records for issuance, such as identifying households that do not have an EBT card or participants requiring a valid food prescription. Staff can then schedule the issuance of benefits via the automated benefit issuance batch process.
- North Carolina Exchange / Increase Formula – This change simplified the formula exchange / increase process by allowing staff to select the functionality they are performing thus improving the precision of the process and workflow for making changes to existing formula benefits.
- Vendor Apps – Voyatek has developed a suite of vendor apps via change requests for the South Dakota and New York WIC Programs, which have subsequently been transferred to NATIONS, Indiana and California WIC programs. The apps are designed to assist state and local vendor teams in managing different aspects of the vendor team's activities. The Retailer mobile app for vendors allows them to upload documents, scan UPCs to determine if they are part of the WIC Approved Product List (APL) and submit shopping incidents for subsequent follow-up by the State. The Vendor Monitoring app and the Vendor Compliance App, both built on the iOS platform and optimized for the iPad, offer vendors and investigation teams essential functionalities by enabling offline data to be captured during in-store activities. These apps synchronize with the MIS system when connected to the network, facilitating the download of cases and the efficient upload of collected information.
- TeleWIC for NATIONS – This CR involved the transfer of the cloud-based telehealth video conferencing solution that Voyatek developed for South Carolina to the ten Indian tribal organizations known collectively as NATIONS.
- Caseload Dashboard – The Caseload Dashboard was initially developed as a change request for Maryland. It has since then been transferred to the systems for the Connecticut and NATIONS WIC Programs with an ongoing effort to integrate it into the California WIC MIS system. This dashboard offers a summary overview of participation levels across the state, with clear and interactive visuals to communicate the caseload positions to include key metrics such as the participant-to-enrollment ratio. Additionally, it provides actionable visuals that enable staff to effectively address issues such as missing participation due to early termination of certification and missing benefit issuances.

f) Defect Corrections

Corrections / defect fixes to correct deficiencies based on the most recently updated published System design documentation (or implemented CRs/estimates where documentation has not yet been updated) are subject to the change request process but at no additional cost.

As stated in the RFP, corrections / defect fixes to correct deficiencies based on the most recently updated published system design documentation (or implemented CRs/estimates where documentation has not yet been updated) are subject to the Change Request Process at no additional cost. Voyatek's approach to defect fixes is summarized in the table shown below and explained in detail in [i\) Describe the Defect / Issue Fix Process](#).

Table 9: Defect Resolution Time by Priority Level

Issue Priority Level	Classification	Priority Description	Issue Resolution Timeframe
1	Critical	Critical Component Failure: Does not allow testing to continue Major malfunction in the System	Within hours
2	Major	Major Component Failure: Does not allow testing to continue Defect or malfunction in certain areas of the System Problem must be resolved	Resolution within one business day
3	Medium	Medium Functional Problem: Testing can continue Functions in certain components do not work properly Components can still work with other components of the System	Resolution within 5 business days or as agreed
4	Minor	Minor Issue: Testing can continue Minor editing error found in a System component	Resolution in the next Planned Release
5	Trivial	Trivial Issue: Testing can continue Design Clarification issue Future enhancement to the System Cosmetic change needed	Not time sensitive, fix as time is available

g) Timely Updates to System Documentation

The Vendor will provide to the State timely updates to appropriate System documentation.

Voyatek will provide the State timely updates to appropriate System documentation. Keeping the system documentation current is a vital part of our stewardship of the Crossroads system. We will update the Crossroads documentation as needed with each system release and provide those updates to North Carolina as part of the release package for review during UAT along with

Release Notes that detail the changes in the release. By so doing, the system documentation updates can be confirmed during UAT so the updates are ready for the release to Production.

h) Documentation Process

Describe the Vendor's process to ensure that appropriate documentation is updated in a timely manner as software changes occur.

Voyatek keeps system documentation up to date by ensuring that documentation is considered with every system enhancement and even some defects. As enhancements are developed, the Business Analyst Manager considered the impact of the associated functionality changes on all system documentation. The documentation is updated in draft and circulated for review by the State before being finalized in time for the UAT. In addition, the Voyatek Quality Assurance Management Plan describes in detail our approach to quality assurance which includes ensuring that the system documentation is updated in a timely manner.

i) Log and Track Change Request Process

Describe the Vendor's process to log and track the status of pending CRs including:

1. The State and Vendor will mutually agree on an assigned sequence number;
2. A short description of the requested change;
3. Whether the change is a table change, code change, or other;
4. The date of the original CR from the State;
5. The date the CR Response was sent to the State;
6. The date the CR Response was approved/not approved by the State;
7. The date the CR Estimate was submitted to the State;
8. The date the CR Estimate was approved/not approved/put on hold by the State;
9. The binding hours and cost of the change;
10. The proposed delivery date for UAT of the completed Change Request;
11. Comments section;
12. Current version of any associated documents;

Voyatek will use Azure DevOps to log and track CRs so that they are visible to the NC-Voyatek team along with defects, organized by release. Each CR will include the information above and tracking of CRs will continue in monthly status reports.

j) Additional Cost Change Requests

For those Change Requests that are at additional cost to be paid by the State, the Vendor's invoice will be processed for payment upon completion and delivery of the Change Request and acceptance of the delivered Change Request by the State. The amount paid for Change Requests will be based on the amount contained in the CR Draft Estimate, signed by the State and the Vendor.

The State will have the option to defer acceptance of a Change Request until the change has been implemented in production, and all required defect corrections found against the Change Request in production have been subsequently implemented into production.

Voyatek acknowledges and agrees with the cost of and payment terms identified above for system change requests.

3.5.13 Technical Upgrades and Environment Validation

Describe the Vendor's approach to recommending technology upgrades and providing environment compatibility / validation services. The services will include, but not be limited to upgrades to hardware infrastructure, operating systems including web browsers, database management systems, and other cloud server or workstation software and hardware to maintain supportable non-production and production environments as third parties release new versions of products, or as current Crossroads components approach end-of-life. Describe how the Vendor will schedule third-party software patches and upgrades to all non-production and production environments through the DHHS Release Manager.

Describe how the Vendor will:

Provide annual written recommendations for upgrades to maintain the Crossroads system and third-party software components, at a version supported by the software vendor and in conformance with North Carolina security and architectural standards. This recommendation will be presented onsite by the Vendor in Raleigh, NC if requested by the State.

Proactively test and validate the Crossroads system for use with the latest release of relevant hardware and software technologies. The testing results and inventory of validated hardware and software will be maintained in the existing System Documentation. Examples of hardware and software to consider include, but are not limited to:

1. Hardware

- a. Scanners;*
- b. Workstation Printers;*
- c. Signature Pads;*
- d. Bar Code Scanners;*
- e. Label Writers;*
- f. EBT Card Readers;*
- g. Lab Equipment such as weight scales, etc.;*
- h. RAM memory requirements, for workstations;*
- i. Disk space requirements for workstations;*
- j. Graphics card requirements*

2. Software

- a. Operating Systems, such as Windows;*
- b. Web Browsers, such as Microsoft Edge;*
- c. Database Management Systems, such as SQL Server;*
- d. .NET Framework and other middleware;*
- e. Web server components;*
- f. Adobe products;*
- g. Microsoft Office products;*
- h. Software Drivers for above Hardware;*
- i. Telehealth frameworks for WIC participant experience*

One of the primary advantages of selecting Voyatek as the maintenance and enhancement vendor will be the continued relationship with the team that has been maintaining NC Crossroads for the past six years as well as working with a company that is the leading vendor for support of WIC MIS systems across the country. Voyatek is currently responsible for recommending and performing technology upgrades for 14 major WIC programs, including all the states that use the Crossroads WIC MIS. Our teams are working steadily on innovative changes for both technical and WIC process improvements within Voyatek MIS systems. As technology capabilities evolve and innovations are developed, we regularly provide status updates and share ideas across our customers. In this proposal, we have presented some of these ideas in the [Appendix R – Optional Services](#).

In addition to the Crossroads project team, Voyatek will utilize architects within our core architecture team when providing system recommendations. The common architecture team assists project teams in recommending and evaluating the impact of technology changes such as upgrades and modernization of:

- Operating systems
- SQL Server, SQL Server Reporting Services, and database driver upgrades
- Development and release management tools
- .Net Framework
- Third-party controls
- Specialized tools we use in maintaining source code and systems

Voyatek will provide annual technology evaluations throughout the contract support period, focusing on advances in technology such as cloud hosting and management, artificial intelligence (AI), and machine learning (ML), all of which are currently altering our technological landscape in dramatic ways. As these and other technologies provide means to reduce costs and/or increase efficiency for our WIC stakeholders, we will share these with NC WIC and collaborate on the best way to take advantage of new capabilities.

For the ongoing management of WIC peripheral hardware, Voyatek maintains a large inventory of scanners, printers, signature pads, bar code scanners, label printers, scanners, EBT card readers, and other equipment to provide testing and driver support for supported states. Our processes include checks for driver updates on North Carolina supported hardware which enables each release test to be performed using the most recent driver upgrades. Any issues identified are recorded in the issue log for prioritization. Voyatek acknowledges the requirement to provide ongoing support for hardware, external interface, and third-party software compatibility.

3.5.14 Contract Transition-Out Procedures

In the event of Contract termination for any reason, non-renewal by the State, or at the expiration of the Contract, the Vendor will be required to provide transition assistance.

Describe a detailed Transition-Out Plan for State review and acceptance, that describes the procedures, detailed schedules, and resources needed to successfully transition services to a new MIS Vendor. Specifications are listed below, in addition to Attachment B: Department of Information Technology Terms and Conditions.

Describe Vendor's Transition-Out Completion Report addressing:

- a) Providing an export of all regression and performance test artifacts, including but not limited to test scripts, test cases, test scenarios, etc.*
- b) Providing a final copy of all source code software, compilation instructions and tools and final updated documentation.*
- c) Providing an export of all issues and file attachments contained in the issue reporting system.*
- d) Providing an export of all action items contained in the action item tracking tool.*
- e) Providing an export of all finalized CR documents, including sample documents and templates that the Vendor has used for the Change Request Process.*
- f) Returning all hardware and software that may be owned by the State upon request by the State. This includes system peripherals and other hardware.*
- g) Maintaining the collaboration web site to allow State staff (or designee) to download artifacts until the Contract expires or is terminated.*
- h) Ensuring that appropriate Vendor development, test, business analyst and other help desk staff are retained until expiration or termination of the Contract.*
- i) Providing technical training to the State (and/or its designee) for eighty (80) hours to include a thorough overview of the system design, including a detailed walkthrough of the source code if requested, at a location to be determined by the State including the incumbent Vendor's facilities. Any unused Supplemental Service Hours may be utilized to provide additional training above these eighty (80) hours if requested by the State. These eighty (80) hours will not include preparation time by the Vendor, or travel time for Vendor staff.*
- j) Describe how the Vendor will assure and confirm that any data or system design provided by or for the State remains the property of the State and may not be marketed or sold by the Vendor without the express written consent of the State.*
- k) Until the Vendor has certified the completion of the data destruction or purge, describe how the Vendor will continue to comply with all data security sections within this RFP, even after the Contract has terminated or expired.*
- l) Describe how Vendor will export or migrate (at the sole discretion of the State) all data (including file systems) from all production and non-production environments into new environments to be determined by the State.*
- m) Describe Vendor's approach to preserving the State's data in the Crossroads 3rd party cloud infrastructure and transferring the Vendor's PaaS or similar service model to the State or its designee, (which the State may request in its sole discretion).*

Voyatek understands the need for a smooth transition between service providers to safeguard against interruption of service to NC WIC or its WIC participants. In the event we are not chosen as the subsequent M&E service provider, we will support a smooth transition to a new M&E provider. Appendix L – Transition-Out Plan provides Voyatek’s commitment to work with the incoming contractor to migrate Crossroads source code and project artifacts into the new contractor’s infrastructure and to support the transition between M&E providers with full cooperation and collaboration. During the Transition-Out period Voyatek will perform the following support services:

- Provide the incoming vendor with a final copy of all system software, compilation instructions and tools, current versions of system documentation, regression and performance test artifacts (test scripts / cases / scenarios, etc.).
- Provide exports of all issues, change requests, action items, etc. along with related files and documents contained in Azure DevOps.
- Migrate production and non-production data from Voyatek’s managed Crossroads infrastructure to the incoming vendor’s platform. The means by which the data will be moved will be determined in collaboration with the incoming vendor and the State. Upon the migration of data to the incoming vendor, Voyatek will maintain all migrated data until such time as the State and incoming vendor confirm a successful migration and that all systems and environments in the incoming vendor’s platform are operating correctly.
- Return hardware and software that is owned by the State (e.g., system peripherals).
- Maintain the SharePoint collaboration web site through the end date of our contract to allow State staff to download artifacts as needed.
- Retain our project team (product manager, developers, quality assurance specialists, business analysts, etc.) through the end date of our contract to provide access to our system and contract knowledge as is needed by the State and/or the incoming contractor.
- Provide technical training to the State and/or the incoming contractor for 80 hours to include a thorough overview of the system design, including a detailed walkthrough of the source code if requested, at a location to be determined by the State including Voyatek facilities, if desired. The 80 hours will not include Voyatek preparation time or travel time for our staff. In addition, we agree that any unused Supplemental Service Hours remaining in the contract may be utilized to provide additional training above the 80 hours.
- Following the transition to the incoming contractor or the State, and upon approval by the State to proceed, Voyatek will destroy all State data in our possession and certify for the State the completion of this process.

In addition to the services above, Voyatek provides the following assurances to North Carolina:

- Voyatek acknowledges that all data and system design provided by or for the State remains the property of the State and will not be marketed or sold by Voyatek without written consent of the State.
- Having been trusted with sensitive data by all our current WIC customers, Voyatek takes the protection of customer sensitive data very seriously. Until the State informs Voyatek to proceed with the destruction of State data in our possession and control, we will continue to be vigilant in the protection of all data associated with the NC WIC contract.

This approach and commitment by Voyatek will provide the lowest risk transition for the State.

3.5.15 North Carolina WIC Program and FMNP Program Data

Describe how the Vendor's proposal can accommodate the following volumes of data

The proposed Voyatek team has experience supporting North Carolina WIC's data volumes and participant caseload since the original development of the Crossroads system. The team understands the importance of system performance to provide efficient participant services and to meet reporting needs.

One key aspect of this support is working to improve and maintain the response speeds within the Crossroads MIS. During the current contract period, Voyatek has worked to significantly improve system performance for system interfaces, Not-To-Exceed (NTE) processing and within reports. The team understands the project SLAs for system response times and has been a strong partner with NC WIC to improve system performance. The system is currently working within expected performance requirements and the Voyatek team will continue to meet these SLAs.

As part of this RFP, Voyatek will assume responsibility for hosting the NC Crossroads system. A key component of that hosting will be to maintain or improve system response times. A key element of this hosting will be the management of North Carolina WIC Program data within the Azure cloud and the Azure SQL Managed Instance. Voyatek is proposing to use a SQL Server managed instance with Premium Series compute and Premium Business Critical tier support. These services are intended to provide North Carolina WIC with a highly performant SQL Server environment with significant advantages over standard services. These advantages include:

- Higher CPU clock speeds for data processing
- More RAM allocated per vCPU
- Specific IOPS allocation per vCPU (4,000/vCPU, for a total of 32,000 IOPS in proposed solution)

- 4 replicas, distributed across availability zones, with included read-only replicas for reporting
- Storage of files and documents will be transitioned to Azure Storage. This storage is intended to greatly improve the reliability of data access and to improve data security with embedded encryption services.
- Geo zone redundant storage (GZRS) in multiple regions within the continental US
- Durable and highly available – Redundancy confirms that your data is safe in the event of transient hardware failures. You can also opt to replicate data across data centers or geographical regions for additional protection from local catastrophe or natural disaster. Data replicated in this way remains highly available in the event of an unexpected outage
- Secure – All data written to an Azure storage account is encrypted by the service. Azure Storage provides you with fine-grained control over who has access to your data
- Scalable – Azure Storage is designed to be massively scalable to meet the data storage and performance needs of today's applications
- Managed – Azure handles hardware maintenance, updates, and critical issues for you.
- Voyatek proposed hosting sizing consistent with or better than existing on-premises hardware – One advantage of using the Azure cloud is that in the event of infrastructure related performance issues, hosting sizing changes can be made easily and quickly. Voyatek staff will utilize Terraform to manage cloud hardware configuration. Terraform allows for the management of hosting configuration changes and the automated deployment of infrastructure upgrades.

3.5.16 Supplemental Services

Provide pricing for Supplemental Service Hours using Attachment D: Cost Form, Cost Table 7: Supplemental Hours, which will be used to document work authorizations via Change Requests to the Crossroads system that are for the account of the State.

The State will allocate up to thirty-five hundred (3500) Supplemental Service Hours Contract Years 1-7 (plus up to an additional five hundred (500) hours for each optional year, if applicable and at the State's discretion) until the end of the Contract term. Unused hours will carry forward to the next year, including optional years that become part of the contract term. Any Change Requests that require more than the Contract's remaining Supplemental Service Hours to complete will be made effective through the Parties' execution of a Contract amendment, implemented in compliance with the rules and practices of DIT Statewide Procurement.

1. Supplemental Service Hours: The aggregate of total Supplemental Service Hours for the entire Contract term will be available to the State beginning in Year 1.

2. Describe the process the Vendor would use for tracking Supplemental Service Hours allocated and expended.

3. Hours for Change Requests required to be performed at no additional cost to the State will not be expended from the Supplemental Services Hours.

Voyatek understands that during the contract period, NC WIC may elect to utilize up to 500 hours per year of software enhancement services and that unused hours in any given year will be carried forward to the following year. Voyatek has experience operating under a similar approach with South Carolina and we have enriched their WoW WIC MIS system with many valuable enhancements over the last seven years. To provide maximum flexibility to the State, the aggregate of the total Supplemental Service Hours for the entire contract term will be available to the State beginning in Year 1 of the contract. The Voyatek product manager will work with the Crossroads WIC MIS Release Manager to manage and report on the utilization of the Supplemental Services Hours pool throughout the contract.

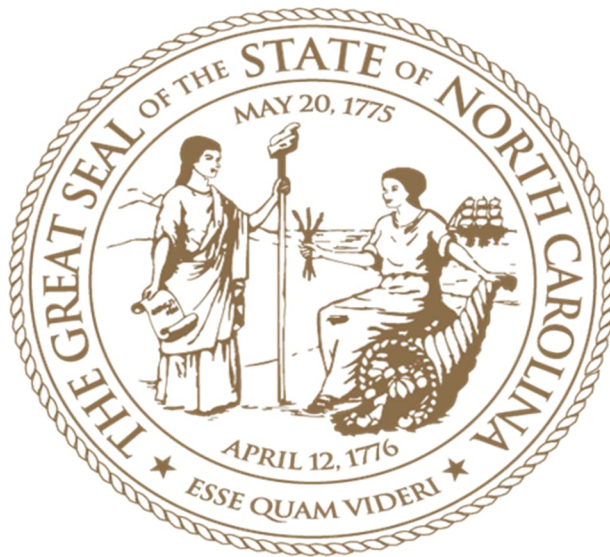
We further understand that the hours for change requests required to be performed at no additional cost to the State will not be drawn down from the Supplemental Services hours. In addition, changes that are needed to fix a defect in an implemented enhancement during the warranty period will not count towards the Supplemental Service hour pool.

To track the allocation and expenditure of Supplemental Service Hours, Voyatek will establish a separate charge number in our internal time tracking system for employees to use whenever they are working on a change that has been designated as a software enhancement using Supplemental Service Hours.

c) Security Vendor Readiness Assessment Report (VRAR)

On the following pages, Voyatek is providing a completed VRAR for the hosting of the Crossroads WIC system in a non-State facility. The VRAR is specific to the architecture and hosting model needed to support the Crossroads system. Voyatek currently has an approved VRAR for the Connects CACFP system and the Crossroads VRAR provided below shares many of the general security and hosting provisions from the existing CACFP VRAR. Voyatek anticipates that approval of the final VRAR will be relatively quick given the shared nature of the hosting models.

ENTERPRISE SECURITY & RISK MANAGEMENT OFFICE (ESRMO)



Vendor Readiness Assessment Report (VRAR) for Solutions Not Hosted on State Infrastructure

Executive Summary

The State of NC requires that all systems connected to the State Network or process State data, meet an acceptable level of security compliance. This includes those systems that operate outside of the States' direct control such as Cloud Services defined as Software as a Service (SaaS), Infrastructure as a Service (IaaS) or Platform as a Service (PaaS).

The State of NC has adopted the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 as the foundation for identifying and implementing information technology security controls. These controls are described in the State of NC Statewide Information Security Manual (SISM).

The following is a high-level view of specific security requirements that are needed to meet compliance. The control references (e.g., AC-2) refer to the specific NIST 800-53 control as listed in the SISM, which may be found at the following link: <https://it.nc.gov/statewide-information-security-policies>.

Note: There may be additional requirements depending on the sensitivity of the data and other Federal and State mandates, or agency specific requirements.

Table of Contents

Executive Summary	i
1. Introduction	1
1.1. Purpose	1
1.2. Outcomes	1
1.3. State Approach and Use of This Document	1
2. VENDOR System Information	2
2.1. Relationship to Other Vendors or CSPs	2
2.2. Data Flow Diagrams	4
2.3. Separation Measures [AC-4, SC-2, SC-7]	4
2.3.1. Pre-Production and Production Environments	5
2.3.2. Physical Separation	5
2.3.3. Logical Separation of System Components	5
2.3.4. User Access	5
2.3.5. Administrative Access	5
2.3.6. Auditing	6
2.4. System Interconnections	6
3. Capability Readiness	8
3.1. State Mandates	8
3.2. State Requirements	9
3.2.1. Data at Rest and Authentication [SC-13]	9
3.2.2. Transport Layer Security [NIST SP 800-52, Revision 2]	9
3.2.3. Identification and Authentication, Authorization, and Access Control	10
3.2.4. Audit, Alerting, Malware, and Incident Response	11
3.2.5. Contingency Planning and Disaster Recovery	13
3.2.6. Configuration and Risk Management	13
3.2.7. Data Center Security	15
3.2.8. Policies, Procedures, and Training	15
3.3. Additional Capability Information	20
3.3.1. Staffing Levels	20
3.3.2. Change Management Maturity	20
3.3.3. Vendor Dependencies and Agreements	20
3.3.4. Continuous Monitoring Capabilities	21
3.3.5. Status of System Security Plan (SSP)	22

List of Tables

Table 2-1. System Information.....	2
Table 2-2. Leveraged Systems.....	2
Table 2-3. Leveraged Services.....	3
Table 2-4. System Interconnections	6
Table 2-5. Interconnection Security Agreements (ISAs).....	7
Table 3-1. State Mandates	8
Table 3-2a. Data at Rest & Authentication	9
Table 3-2b. Transport Encryption.....	9
Table 3-3. Transport Protocol	9
Table 3-4. Identification and Authentication, Authorization, and Access Control.....	10
Table 3-5. Audit, Alerting, Malware, and Incident Response	11
Table 3-6. Contingency Planning and Disaster Recovery.....	13
Table 3-7. Configuration and Risk Management.....	13
Table 3-8. Data Center Security.....	15
Table 3-9. Policies and Procedures.....	16
Table 3-10. Missing Policy and Procedure Elements.....	19
Table 3-11. Security Awareness Training.....	19
Table 3-12. Staffing Levels	20
Table 3-13. Change Management	20
Table 3-14. Vendor Dependencies and Agreements.....	20
Table 3-15. Vendor Dependency Details	21
Table 3-16. Formal Agreements Details	21
Table 3-17. Continuous Monitoring Capabilities.....	21
Table 3-18. Continuous Monitoring Capabilities – Additional Details.....	22
Table 3-19. Maturity of the System Security Plan.....	22
Table 3-20. Controls Designated “Not Applicable”	22
Table 3-21. Controls with an Alternative Implementation	22

1. Introduction

1.1. Purpose

This report and its underlying assessment are intended to enable State agencies to reach a state-ready decision for a specific system not hosted on the State of NC's infrastructure that is based on organizational processes and the security capabilities of the Moderate/Low-impact information system.

1.2. Outcomes

Submission of this report by the Vendor does not guarantee a state-ready designation, nor does it guarantee that the State will procure services from the vendor.

1.3. State Approach and Use of This Document

The VRAR identifies clear and objective security capability requirements, where possible, while also allowing for the presentation of more subjective information. The clear and objective requirements enable the vendor to concisely identify whether an application or vendor is achieving the most important State Moderate or Low baseline requirements. The combination of objective requirements and subjective information enables State to render a readiness decision based on a more complete understanding of the vendor's security capabilities.

Section 4, Capability Readiness, is organized into three sections:

- Section 3.1, State Mandates, identifies a small set of the state mandates a vendor must satisfy. State will not waive any of these requirements.
- Section 3.2, State Requirements, identifies an excerpt of the most compelling requirements from the National Institute of Science and Technology (NIST) Special Publication (SP) 800 document series and State guidance. A VENDOR is unlikely to achieve approval if any of these requirements are not met.
- Section 3.3, Additional Capability Information, identifies additional information that is not tied to specific requirements, yet has typically reflected strongly on a VENDOR's ability to achieve approval.

2. VENDOR System Information

Provide and validate the information below. For example, if the deployment model is Government only, ensure there are no non-Government customers. The VRAR template is intended for systems categorized at the Moderate or Low security impact level, in accordance with the FIPS Publication 199 Security Categorization.

Table 2-1. System Information

VENDOR Name: Voyatek
Solution/System Name: Crossroads
Service Model: (IaaS, PaaS)
FIPS PUB 199 System Security Level: (e.g., Moderate)
Fully Operational as of: To be determined, not currently operational
Number of Customers (State/Others): North Carolina
Deployment Model: Azure Commercial Cloud
System Functionality: The Crossroads system is a management information system designed for WIC programs developed by North Carolina in conjunction with Federal funds.

2.1. Relationship to Other Vendors or CSPs

If this system resides in another VENDOR's environment or inherits security capabilities, please provide the relevant details in Tables 2-2 and 2-3 below. Please note, the leveraged system itself must be State Authorized. For example, a large VENDOR may have a commercial service offering and a separate service offering with a State Authorization. Only the service offering with the State Authorization may be leveraged.

IMPORTANT: If there is a leveraged system, be sure to note below every capability that partially or fully leverages the underlying system. When doing so, indicate the capability is fully inherited or describe both the inherited and non-inherited aspects of the capability.

Table 2-2. Leveraged Systems

#	Question	Yes	No	N/A	If Yes, please describe.
1	Is this system leveraging an underlying provider?				The system will be hosted in the Microsoft Azure Commercial Cloud. The system utilizes several PaaS and IaaS services in the Azure environment, such as Azure SQL Managed Instance. Some network management duties, such as traffic management/routing, edge firewalls, and reverse proxying, will be handled by Fortigate software deployed to the cloud environment.

List all services leveraged. The system from which the service is leveraged must be listed in Table 2-2 above.

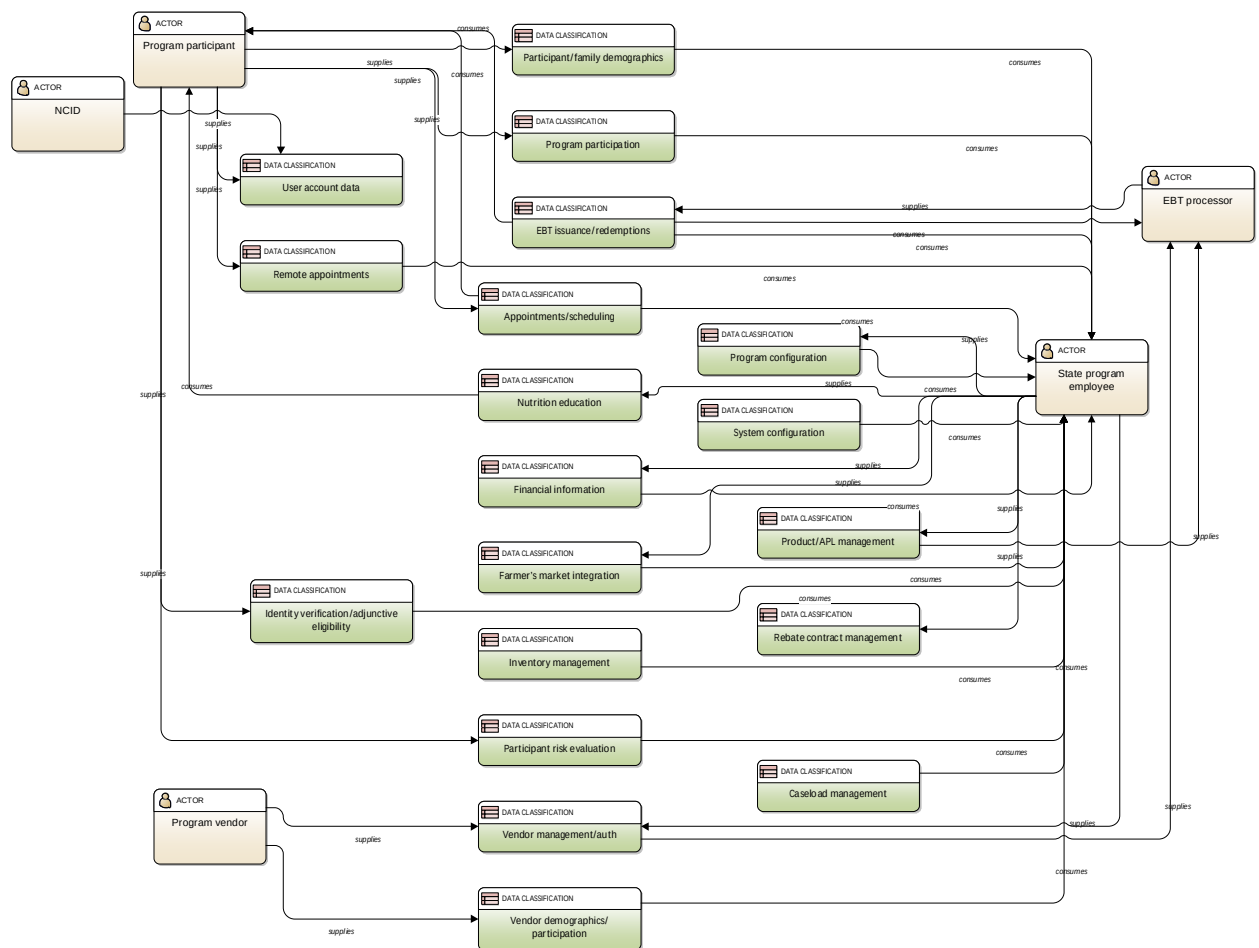
Table 2-3. Leveraged Services

#	Service	Service Capability	System
1	<i>State what is being leveraged or "None" if no service is leveraged or if the VENDOR is responsible for the entire stack.</i>	<i>Database</i>	<i>Azure SQL Managed Instance</i>
		<i>Network traffic management</i>	<i>Fortigate</i>

2.2. Data Flow Diagrams

Insert Vendor-validated data flow diagram(s) and provide a written description of the data flows. The diagram(s) must:

- clearly identify anywhere State data is to be processed, stored, or transmitted;
- clearly delineate how data comes into and out of the system boundary;
- clearly identify data flows for privileged, non-privileged and customer access; and
- depict how all ports, protocols, and services of all inbound and outbound traffic are represented and managed.



2.3. Separation Measures [AC-4, SC-2, SC-7]

Assess and describe the strength of the physical and/or logical separation measures in place to provide segmentation and isolation of tenants, administration, and operations; addressing user-to-system; admin-to-system; and system-to-system relationships.

The Vendor must base the assessment of separation measures on very strong evidence, such as the review of any existing penetration testing results, or an expert review of the products, architecture, and configurations involved. The Vendor must describe how the methods used to verify the strength of separation measures.

2.3.1. Pre-Production and Production Environments

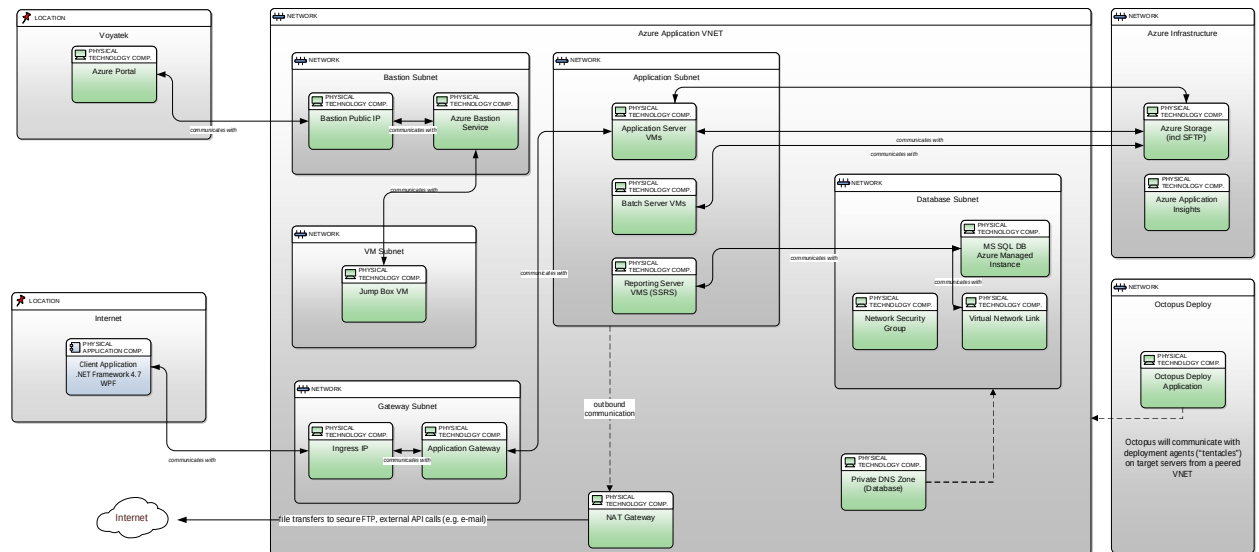
The system's pre-production and production environments are entirely separate and do not share any common elements. This includes networks, cloud IaaS and/or PaaS services, virtual machines, and containers. Admin access to each environment is also separate; the two environments do not share the same cloud subscription.

2.3.2. Physical Separation

Pre-production environments share a physical environment. The production environment is, as mentioned above, physically separate, from both administrative and deployment perspectives.

2.3.3. Logical Separation of System Components

The pre-production and production system architectures are identical in structure. Each uses isolated virtual networks and subnets so that system components are not directly accessible over the Internet. The network diagram below shows how the cloud network is divided into subnets for different areas of the system.



2.3.4. User Access

User access to the system is always handled via an application gateway that controls traffic flow. The gateway only allows HTTPS traffic in and out. Because the virtual network and subnets where the application is deployed are private, the gateway is the only way for traffic to pass from the Internet to the back-end application services. The gateway does not provide access to any other system components other than the API and the client (so that it can be downloaded and run on user's computers).

2.3.5. Administrative Access

Since the system is cloud-hosted, all administrative access is handled by the Azure portal. Via the portal, administrators can view and manage configuration settings, enable/disable services, read system logs, and perform other diagnostic activities. The pre-production environment is accessible to senior developers, technical leads, and architects. The main use for this access is to see logging and system configuration

information to troubleshoot issues that arise during development. A few components, like the key vault (which stores the SSL certificates the application gateway uses) are not accessible to administrative users without explicit special permission being granted.

The production environment is only accessible by a few people who have need for direct administrative access. Currently, this only includes select staff who work in managed services (and who are assigned to work on this system) as well as the system's lead architect, who designed the deployment environment. Developers do not have access to the production system at all. In addition, administrative access roles and permissions are handled by Azure Active Directory, and the directory is entirely separate from the main corporate directory used by VOYATEK. Federated accounts from the main corporate directory are used to manage access. This allows the convenience of being able to disable accounts from either directory (for example, if a person leaves VOYATEK employment) while keeping role assignments and admin access separate and isolated.

2.3.6. Auditing

VOYATEK's SOC 2 audit covers environment design for cloud-hosted systems.

2.4. System Interconnections

A System Interconnection is a dedicated connection between information systems, such as between a SaaS/PaaS and underlying IaaS.

The Vendor must complete the table below. If the answer to any question is "yes," please briefly describe the connection. Also, if the answer to the last question is "yes," please complete Table 2-5 below.

Table 2-4. System Interconnections

#	Question	Yes	No	If Yes, please describe.
1	Does the system connect to the Internet?	X		Crossroads is a client server application (deployed using Microsoft's ClickOnce technology) and third-party facing web portals that provides access to NC State staff, authorized local agencies, WIC participants and authorized vendors.
2	Does the system connect to a corporate or state infrastructure/network?	X		The NCID system is used to authenticate users.
3	Does the system connect to external systems?	X		System performs file transfers via SFTP (FTP over SSH) and web services to deliver files to the State's EBT processor CDP.

If there are connections to external systems, please list each in the table below, using one row per interconnection. If there are no external system connections, please type "None" in the first row.

Table 2-5. Interconnection Security Agreements (ISAs)

#	External System Connection	Does an ISA Exist?		Interconnection Description. If no ISA, please justify below.
		Yes	No	
1	CDP FTP	X		Voyatek assumes NC maintains this with their contracted vendor CDP.
2	CDP Web Services	X		Voyatek assumes NC maintains this with their contracted vendor CDP.
3	North Carolina CNDS	X		The system connects to the North Carolina Common Name Data Services
4	Teletask	X		Voyatek assumes NC maintains this with their contracted vendor.

3. Capability Readiness

3.1. State Mandates

This section identifies State requirements applicable to all State approved systems. All requirements in this section must be met. Some of these topics are also covered in greater detail in Section 3.2, *State Requirements*, below.

Only answer "Yes" if the requirement is fully and strictly met. The Vendor must answer "No" if an alternative implementation is in place.

Table 3-1. State Mandates

#	Compliance Topic	Fully Compliant?	
		Yes	No
1	Data at Rest, Authentication: Are FIPS 140-2/-3 Validated or National Security Agency (NSA)-Approved cryptographic modules only used where cryptography is required?	X	
2	Transmission, Remote Access: Are FIPS 140-2/-3 Validated or National Security Agency (NSA)-Approved cryptographic modules consistently used where cryptography is required?	X	
3	Can the VENDOR'S solution integrate with the State's NCID solution?	X	
4	Does the VENDOR utilize security boundary/threat protection devices to protect the network, system, application...e.g., firewalls intrusion detection/prevention systems, end point protection etc.? [SC-7] [SI-3/SI-4]	X	
5	Does the VENDOR have the ability to consistently remediate High risk vulnerabilities within 30 days and Medium risk vulnerabilities within 60 days? [SI-2]	X	
6	Does the VENDOR and system meet Federal Records Management Requirements, including the ability to support record holds, National Archives and Records Administration (NARA) requirements, and Freedom of Information Act (FOIA) requirements?	X	
7	Does the VENDOR store, process or transmit <u>State data</u> only in the continental US and is that data backed up in only US locations?	X	
8	Does the VENDOR have a process to securely dispose of State data from its systems upon request that is in accordance with the National Institute for Standards and Technology (NIST) Special Publication 800-88 revision 1 <u>and</u> will provide to the State a certificate of data destruction? [MP-6]	X	
9	All operating systems (OS) <u>AND</u> major application software components (e.g., Microsoft SQL, Apache Tomcat, Oracle Weblogic, etc.), must NOT be past N-1. Applications which are not operating on the most recent platform MUST have a roadmap to upgrade with a State approved timeline. Does the application support the N-1 requirement?	X	
10	Does the vendor have a current 3 rd party attestation certification <u>and</u> is it regularly renewed? The State requires an independent 3 rd party attestation (e.g., FedRAMP, SOC 2 Type 2, ISO 27001, or HITRUST) <i>prior to</i> contract award for systems containing Restricted/Highly Restricted data. <i>Note: SaaS vendors cannot use IaaS/PaaS certification unless the application is explicitly covered as part of the IaaS/PaaS assessments.</i> [CA-7, RA-3, SA-9]	X	

11	Does the VENDOR's staff have appropriate background checks for unprivileged and privileged access and accounts according to Federal and/or State designation procedures for those systems that require it? [AC-2, PS-3]	X	

3.2. State Requirements

This section identifies additional State Readiness requirements. All requirements in this section must be met; however, alternative implementations and non-applicability justifications may be considered on a limited basis.

3.2.1. Data at Rest and Authentication [SC-13]

The Vendor must ensure FIPS 140-2, or 140-3 where available, Validated or NSA-Approved algorithms are used for all encryption modules. FIPS 140-2 Compliant is not sufficient. The Vendor may add rows to the table if appropriate but must not remove the original rows. The Vendor must identify all non-compliant cryptographic modules in use.

Table 3-2a. Data at Rest & Authentication

	Cryptographic Module Type	FIPS 140-2 Validated?		NSA Approved?		Describe Any Alternative Implementations (if applicable)	Describe Missing Elements or N/A Justification
		Yes	No	Yes	No		
1	Data at Rest [SC-28]	X		X			
2	Authentication [IA-5, IA-7]	X		X			

3.2.2. Transport Layer Security [NIST SP 800-52, Revision 2]

The Vendor must ensure FIPS 140-2, or 140-3 where available, Validated or NSA-Approved algorithms are used for all encryption modules relating to block ciphers, digital signatures and hash functions. Full FIPS mode is not required unless other regulatory requirements must be met. The Vendor may add rows to the table if appropriate but must not remove the original rows. The Vendor must identify all non-compliant cryptographic modules in use.

Table 3-2b. Transport Encryption

	Cryptographic Module Type	FIPS 140-2 Validated?		NSA Approved?		Describe Any Alternative Implementations (if applicable)	Describe Missing Elements or N/A Justification
		Yes	No	Yes	No		
1	Transmission [SC-8 (1), SC-12, SC-12 (2, 3)]	X		X			
2	Remote Access [AC-17 (2)]	X		X			

The Vendor must identify all protocols in use. The Vendor may add rows to the table if appropriate, but must not remove the original rows.

Table 3-3. Transport Protocol

#	The Cryptographic Module Type	Protocol In Use?		If "yes," please describe use for both internal and external communications
		Yes	No	
1	SSL (Non-Compliant)			

2	TLS 1.0 (Non-Compliant)			
3	TLS 1.1 (Non-Compliant)			
4	TLS 1.2 (Compliant)	X		TLS 1.2 is used to secure external access (from users to the edge of the cloud network) and for inter-system communication.
5	TLS 1.3 (Compliant)			

3.2.3. Identification and Authentication, Authorization, and Access Control

Only answer “yes” if the answer is consistently “yes.” For partially implemented areas, answer “no” and describe what is missing to achieve a “yes” answer. If inherited, please indicate partial or full inheritance in the “Describe Capability” column. Any non-inherited capabilities must be described.

Table 3-4. Identification and Authentication, Authorization, and Access Control

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
1	Does the system uniquely identify and authorize organizational users (or processes acting on behalf of organizational users) in a manner that cannot be repudiated, and which sufficiently reduces the risk of impersonation? [IA-2, IA-4]	X		User identity will be provided to the system via NCID integration/login.
2	Does the system require multi-factor authentication (MFA) for administrative accounts and functions? [IA-2, IA-2 (1), IA-2 (2)]	X		Authentication is controlled by NCID for end-user logins to the system itself. Azure Active Directory is used to process user authentication requests for administrative connections to Azure. MFA is required for all admin accounts.
3	Is role-based access used, managed, and monitored? [IA-4, IA-5]	X		Role-based security is supported.
4	Does the system restrict non-authorized personnel’s access to resources? [AC-6, AC-6 (1), AC-6 (2)]	X		Users are required to log in. Role-based security access controls limit access to only functions users are authorized to perform.
5	Does the system restrict non-privileged users from performing privileged function? [AC-6, AC-6 (1), AC-6 (2), AC-6 (10)]	X		Users are required to log in. Role-based security access controls limit access to only functions users are authorized to perform.
6	Does the system ensure secure separation of customer data? [SC-4]	X		North Carolina will have a dedicated instance in every environment. No elements will be shared with other entities.
7	Does the system ensure secure separation of customer processing environments? [SC-2]	X		In the production environment, no resources are shared with any other customer and deployment environments are not connected between customers.

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
8	Does the system restrict access of administrative personnel in a way that limits the capability of individuals to compromise the security of the information system? [AC-2]	X		Cloud hosting environments are deployed and maintained using Terraform and automated deployments. Access to virtual machines that comprise the system environment is limited to a small number of administrative users. Remote desktop connections to the servers must be done via a bastion service controlled by the cloud hosting provider. Users must authentication with MFA to the cloud hosting provider and provide machine credentials to log in.
9	Does the remote access capability include VENDOR-defined and implemented usage restrictions, configuration guidance, and authorization procedure? [AC-17]	X		Yes, user access to the deployed environment in Azure is controlled and limited to specified users.
10	How will the State's password policy be enforced? State requires minimum 14-character complex passwords (Upper, Lower, Special Character & Numerical) [IA-5]	X		Password policy is enforced by NCID and is outside the control of the system.

3.2.4. Audit, Alerting, Malware, and Incident Response

Only answer "yes" if the answer is consistently "yes." For partially implemented areas, answer "no" and describe what is missing to achieve a "yes" answer. If inherited, please indicate partial or full inheritance in the "Describe Capability" column. Any non-inherited capabilities must be described.

Table 3-5. Audit, Alerting, Malware, and Incident Response

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
1	Does the system have the capability to detect, contain, and eradicate malicious software? [SI-3]	X		Virtual machines are enrolled in management software to automatically apply patches and remove malicious software.
2	Does the system store audit data in a tamper-resistant manner which meets chain of custody and any e-discovery requirements? [AU-4, AU-9]	X		Changes to system data are tracked for each table in the database. These detailed audit records are generated and stored at the time of each change.
3	Does the VENDOR have the capability to detect unauthorized or malicious use of the system, including insider threat and external intrusions? [SI-4, SI-4 (4), SI-4 (5), SI-7, SI-7 (7)]	X		System configuration is managed by Octopus, Terraform, and other cloud management tools such as Windows Defender (running in Azure). These tools can provide alerts if system configuration changes are made outside the automated deployment process.

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
4	Does the VENDOR log and monitor access to the system? [SI-4]	X		Azure logs access to infrastructure via the Azure portal or command-line interface. Deployments to infrastructure are logged (both software and infrastructure deployments are automated in Azure DevOps, Octopus, and Terraform)
5	Does the VENDOR have an Incident Response Plan and a fully developed Incident Response test plan? [IR-3, IR-8]	X		Yes, confirmation of the plan is part of SOC II audit controls
6	Does the VENDOR have a plan and capability to perform security code analysis and assess code for security flaws, as well as identify, track, and remediate security flaws? [SA-11]	X		Yes, Microfocus Fortify On Demand is used for code and security analysis.
7	Does the VENDOR implement automated mechanisms for incident handling and reporting? [IR-4, IR-4 (1), IR-6]	X		VOYATEK plans to use the Azure DevOps ALM tool to capture and record incident data, communicate status, and provide reporting data.
8	Does the VENDOR retain online audit records for at least 90 days to provide support for after-the-fact investigations of security incidents and offline for at least one year to meet regulatory and organizational information retention requirements? [AU-11]	X		
9	Does the VENDOR have the capability to notify customers and regulators of confirmed incidents in a timeframe consistent with all legal, regulatory, or contractual obligations? The State of NC's requirement for security breach reporting is 24 hrs. of incident confirmation. [IR-6]	X		Yes, these are documented within the Incident Reporting Plan and monitored within SOC II controls.
10	If the VENDOR's solution provides email "send as" capabilities, does it support DMARC and DKIM for email protection?	X		

3.2.5. Contingency Planning and Disaster Recovery

Only answer “yes” if the answer is consistently “yes.” For partially implemented areas, answer “no” and describe what is missing to achieve a “yes” answer. If inherited, please indicate partial or full inheritance in the “Describe Capability” column. Any non-inherited capabilities must be described.

Table 3-6. Contingency Planning and Disaster Recovery

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
1	Does the VENDOR have the capability to recover the system to a known and functional state following an outage, breach, DoS attack, or disaster? [CP-2, CP-9, CP-10]	X		Database service is zone redundant at minimum—a standby server is always available within another zone in the same region as the primary server. The state can request additional redundancy for the database if desired. File storage for documents is globally redundant (Azure GZRS tier).
2	Does the VENDOR have a Contingency Plan and a fully developed Contingency Plan test plan in accordance with Statewide Information Security Manual? [CP-2, CP-4]	X		
3	Does the system have alternate storage and processing facilities? [CP-6, CP-7]	X		Database service is zone redundant at minimum—a standby server is always available within another zone in the same region as the primary server. The state can request additional redundancy for the database if desired. File storage for documents is globally redundant (Azure GZRS tier).
4	Does the system have or use alternate telecommunications providers? [CP-8]	X		Azure maintains alternative telecommunication providers.
5	Does the system have backup power generation or other redundancy? [PE-11]	X		Yes, the cloud provider provides this capability in their environment.
6	Does the VENDOR have service level agreements (SLAs) in place with all telecommunications providers? [CP-8]		X	N/A

3.2.6. Configuration and Risk Management

Only answer “yes” if the answer is consistently “yes.” For partially implemented areas, answer “no” and describe what is missing to achieve a “yes” answer. If inherited, please indicate partial or full inheritance in the “Describe Capability” column. Any non-inherited capabilities must be described.

Table 3-7. Configuration and Risk Management

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
1	Does the VENDOR maintain a current, complete, and accurate baseline configuration of the information system? [CM-2]	X		Yes, all configuration is managed in Terraform (for cloud infrastructure) and Octopus (for system configuration).

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
2	Does the VENDOR maintain a current, complete, and accurate inventory of the information system software, hardware, and network components? [CM-8]	X		Various artifacts are used to capture this data, such as diagrams, spreadsheets, and deployment templates used with the cloud hosting provider.
3	Does the VENDOR have a Configuration Management Plan? [CM-9]	X		
4	Does the VENDOR follow a formal change control process that includes a security impact assessment? [CM-3, CM-4, CM-4 (2)]	X		
5	Does the VENDOR employ automated mechanisms to detect inventory and configuration changes? [CM-2, CM-2 (2), CM-6, CM-8]	X		Terraform is used to detect and correct environment drift, including configuration settings changes. Octopus deployments reset any environmental changes to specified values during deployments.
6	Does the VENDOR prevent unauthorized changes to the system? [CM-5]	X		VOYATEK would be in full control of deployments to the system environments and does not allow unauthorized users to access the system.
7	Does the VENDOR establish configuration settings for products employed that reflect the most restrictive mode consistent with operational requirements? [CM-6, CM-7]	X		Yes. Zero-trust principles are followed in regards to connectivity and networking. Private endpoints are used for most services to avoid publicly exposing endpoints.
8	Does the VENDOR ensure that checklists for configuration settings are Security Content Automation Protocol (SCAP)-validated or SCAP-compatible (if validated checklists are not available)? [CM-6]		X	No

For the following questions, Vendors may use Table 3-18 “Continuous Monitoring Capabilities – Additional Details” to enter the capability descriptions, supporting evidence, and missing elements.

9	Does the VENDOR perform authenticated operating system/ infrastructure, web, and database vulnerability scans at least monthly, as applicable? [RA-5, RA-5 (5)]	X		Microsoft Azure performs scans on database and infrastructure. Voyatek performs scans within the hosted environments.
10	Does the VENDOR demonstrate the capability to remediate High risk vulnerabilities within 30 days and Moderate risk vulnerabilities within 60 days? [RA-5, SI-2]	X		

11	When a High risk vulnerability is identified as part of continuous monitoring activities, does the VENDOR consistently check audit logs for evidence of exploitation? [RA-5]	X		
12	Does the VENDOR have a Supply Chain Risk Management (SCRM) plan and processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of information systems?	X		<i>Describe the Vendor's SCRM plan and processes.</i>

3.2.7. Data Center Security

Only answer "yes" if the answer is consistently "yes." For partially implemented areas, answer "no" and describe what is missing to achieve a "yes" answer. If inherited, please indicate partial or full inheritance in the "Describe Capability" column. Any non-inherited capabilities must be described.

Table 3-8. Data Center Security

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
1	Does the VENDOR restrict physical system access to only authorized personnel? [PE-2 through PE-6, PE-8]		X	Physical access to infrastructure is controlled by the hosting provider (Azure).
2	Does the VENDOR monitor and log physical access to the information system, and maintain access records? [PE-6, PE-8]		X	These records are maintained by the cloud hosting provider.
3	Does the VENDOR monitor and respond to physical intrusion alarms and surveillance equipment? [PE-6, PE-6 (1)]		X	This would be handled by the cloud provider.

3.2.8. Policies, Procedures, and Training

The Vendor must indicate the status of policy and procedure coverage for the NIST 800-53 Rev 5 families listed in Table 3-9 below.

To answer "yes" to a policy, it must be fully developed, documented, and disseminated; and it must address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. A single policy document may address more than one family provided the NIST requirements of each "-1" are fully addressed.

To answer "yes" to a procedure, it must be fully developed and consistently followed by the appropriate staff. List all applicable procedure documents for each family.

VENDORS must establish their own set of Policies and Procedures (P&Ps). They cannot be inherited from a leveraged system, nor can they be provided by the customer. Any exceptions and/or missing policy and procedure elements must be explained in Table 3-10 below.

Table 3-9. Policies and Procedures

#	Family	Policy		Procedure		Title Version and Date
		Yes	No	Yes	No	
1	Access Control [AC-1]	X		X		VOYATEK maintains a SOC-2 audit for hosting and development environments. VOYATEK additionally maintains a hosting security plan, policies, and other documentation necessary to meet requirements. These can be mapped as needed following contract award. •
2	Awareness & Training [AT-1]	X		X		VOYATEK maintains a SOC-2 audit for hosting and development environments. VOYATEK additionally maintains a hosting security plan, policies, and other documentation necessary to meet requirements. These can be mapped as needed following contract award. •
3	Audit & Accountability [AU-1]	X		X		VOYATEK maintains a SOC-2 audit for hosting and development environments. VOYATEK additionally maintains a hosting security plan, policies, and other documentation necessary to meet requirements. These can be mapped as needed following contract award. •
4	Security Assessment & Authorization [CA-1]	X		X		VOYATEK maintains a SOC-2 audit for hosting and development environments. VOYATEK additionally maintains a hosting security plan, policies, and other documentation necessary to meet requirements. These can be mapped as needed following contract award. •
5	Configuration Management [CM-1]	X		X		VOYATEK maintains a SOC-2 audit for hosting and development environments. VOYATEK additionally maintains a hosting security plan, policies, and other documentation necessary to meet requirements. These can be mapped as needed following contract award. •

#	Family	Policy		Procedure		Title Version and Date
		Yes	No	Yes	No	
6	Contingency Planning [CP-1]	X		X		VOYATEK maintains a SOC-2 audit for hosting and development environments. VOYATEK additionally maintains a hosting security plan, policies, and other documentation necessary to meet requirements. These can be mapped as needed following contract award. •
7	Identification & Authentication [IA-1]	X		X		VOYATEK maintains a SOC-2 audit for hosting and development environments. VOYATEK additionally maintains a hosting security plan, policies, and other documentation necessary to meet requirements. These can be mapped as needed following contract award. •
8	Incident Response [IR-1]	X		X		VOYATEK maintains a SOC-2 audit for hosting and development environments. VOYATEK additionally maintains a hosting security plan, policies, and other documentation necessary to meet requirements. These can be mapped as needed following contract award. •
9	Maintenance [MA-1]	X		X		VOYATEK maintains a SOC-2 audit for hosting and development environments. VOYATEK additionally maintains a hosting security plan, policies, and other documentation necessary to meet requirements. These can be mapped as needed following contract award. •
10	Media Protection [MP-1]	X		X		VOYATEK maintains a SOC-2 audit for hosting and development environments. VOYATEK additionally maintains a hosting security plan, policies, and other documentation necessary to meet requirements. These can be mapped as needed following contract award. •
11	Physical & Environmental Protection [PE-1]	X		X		VOYATEK maintains a SOC-2 audit for hosting and development environments. VOYATEK additionally maintains a hosting security plan, policies, and other documentation necessary to meet requirements. These can be mapped as needed following contract award. •

#	Family	Policy		Procedure		Title Version and Date
		Yes	No	Yes	No	
12	Personnel Security [PS-1]	X		X		VOYATEK maintains a SOC-2 audit for hosting and development environments. VOYATEK additionally maintains a hosting security plan, policies, and other documentation necessary to meet requirements. These can be mapped as needed following contract award. •
13	Risk Assessment [RA-1]	X		X		VOYATEK maintains a SOC-2 audit for hosting and development environments. VOYATEK additionally maintains a hosting security plan, policies, and other documentation necessary to meet requirements. These can be mapped as needed following contract award. •
14	System & Services Acquisition [SA-1]	X		X		VOYATEK maintains a SOC-2 audit for hosting and development environments. VOYATEK additionally maintains a hosting security plan, policies, and other documentation necessary to meet requirements. These can be mapped as needed following contract award. •
15	System & Communications Protection [SC-1]	X		X		VOYATEK maintains a SOC-2 audit for hosting and development environments. VOYATEK additionally maintains a hosting security plan, policies, and other documentation necessary to meet requirements. These can be mapped as needed following contract award. •
16	System & Information Integrity [SI-1]	X		X		VOYATEK maintains a SOC-2 audit for hosting and development environments. VOYATEK additionally maintains a hosting security plan, policies, and other documentation necessary to meet requirements. These can be mapped as needed following contract award. •
17	Planning [PL-1]	X		X		VOYATEK maintains a SOC-2 audit for hosting and development environments. VOYATEK additionally maintains a hosting security plan, policies, and other documentation necessary to meet requirements. These can be mapped as needed following contract award.

#	Family	Policy		Procedure		Title Version and Date
		Yes	No	Yes	No	
18	Supply Chain Risk Management [SR-1]	X		X		VOYATEK maintains a SOC-2 audit for hosting and development environments. VOYATEK additionally maintains a hosting security plan, policies, and other documentation necessary to meet requirements. These can be mapped as needed following contract award.

For any family with a policy or procedure gap, please describe the gap below.

Table 3-10. Missing Policy and Procedure Elements

Missing Policy and Procedure Elements
•

The Vendor must answer the questions below.

Table 3-11. Security Awareness Training

Question	Yes	No	Describe capability, supporting evidence, and any missing elements
Does the VENDOR train personnel on security awareness and role-based security responsibilities? [AT-2]	X		Training documentation and auditing is part of the existing SOC 2 report. VOYATEK staff receive annual security training.

3.3. Additional Capability Information

State will evaluate the responses in this section on a case-by-case basis relative to a State-Ready designation decision.

3.3.1. Staffing Levels

In the table below, the Vendor must describe the VENDOR's organizational structure, staffing levels currently dedicated to the security of the system, as well as any planned changes to these staffing levels. This description must clearly indicate role and number of individuals as well as identify which staff is full-time dedicated, and which are performing their role as a collateral duty. Note: It is not necessary to include specific names of individuals, but rather their roles/titles.

Table 3-12. Staffing Levels

Staffing Levels	
VOYATEK has a full time CISO with two full time Security Engineers who maintain Cyber Security Policy and Procedures as well as audit compliance with those NIST 800.53 R5 based Policies and Procedures. VOYATEK has an Operations Center staffed 24x7 with 12 Analysts and 1 Sr. Manager responsible for operating a SIEM tool for monitoring and escalation of alerts (security & other) and following incident\problem management procedures. Additionally, VOYATEK utilizes a 3rd party Security Operations Center(SOC) that receives security only alerts and analyzes them for anomalies, trends, impact and risk.	

3.3.2. Change Management Maturity

While the following change management capabilities are not required, they indicate a more mature change management capability and may influence a State Readiness decision, especially for larger systems.

The Vendor must answer the questions below.

Table 3-13. Change Management

#	Question	Yes	No	If "no", please describe how this is accomplished.
1	Does the VENDOR's change management capability include a fully functioning Change Control Board (CCB)?	X		
2	Does the VENDOR have and use development and/or test environments to verify changes before implementing them in the production environment?	X		

3.3.3. Vendor Dependencies and Agreements

The Vendor must answer the questions below.

Table 3-14. Vendor Dependencies and Agreements

#	Question	Yes	No	Instructions
1	Does the system have any dependencies on other vendors such as a leveraged service offering, hypervisor and operating system patches, physical security and/or software and hardware support?	X		Native Azure cloud management capabilities are used for patching, physical security.

#	Question	Yes	No	Instructions
2	Within the system, are all products still actively supported by their respective vendors?	X		VOYATEK will only utilize actively supported products; if the transfer system uses outdated components, they will be upgraded if possible.
3	Does the VENDOR have a formal agreement with a vendor, such as for maintenance of a leveraged service offering?	X		Engagement with the cloud service provider would be covered by a service agreement between either VOYATEK and the CSP (if services are procured through VOYATEK) or between the state and the CSP (if services are procured through the state).

If there are vendor dependencies, please list each in the table below, using one row per dependency. For example, if using another vendor's operating system, list the operating system, version, and vendor name in the first column, briefly indicate the VENDOR's reliance on that vendor for patches, and indicate whether the vendor still develops and issues patches for that product. If there are no vendor dependencies, please type "None" in the first row.

Table 3-15. Vendor Dependency Details

#	Product and Vendor Name	Nature of Dependency	Still Supported?	
			Yes	No
1	Azure Cloud	Cloud hosting provider	X	
2				

If there are formal vendor agreements in place, please list each in the table below, using one row per agreement. If there are no formal agreements, please type "None" in the first row.

Table 3-16. Formal Agreements Details

#	Organization Name	Nature of Agreement
1	None	
2		

3.3.4. Continuous Monitoring Capabilities

In the tables below, please describe the current state of the VENDOR's Continuous Monitoring capabilities, as well as the length of time the VENDOR has been performing Continuous Monitoring for this system.

Table 3-17. Continuous Monitoring Capabilities

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
1	Does the VENDOR have a lifecycle management plan that ensures products are updated before they reach the end of their vendor support period?	X		

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
2	Does the VENDOR have the ability to scan all hosts in the inventory?	X		VMs are regularly scanned.
3	Does the VENDOR have the ability to provide scan files in a structure data format, such as CSV, XML files?	X		
4	Is the VENDOR properly maintaining their Plan of Actions and Milestones (POA&M), including timely, accurate, and complete information entries for new scan findings, vendor check-ins, and closure of POA&M items?	X		

In the table below, provide any additional details the Vendor believes to be relevant to State's understanding of the VENDOR's Continuous Monitoring Capabilities. If the Vendor has no additional details, please state, "None."

Table 3-18. Continuous Monitoring Capabilities – Additional Details

Continuous Monitoring Capabilities – Additional Details
Can the vendor provide a current 3rd party attestation certification <u>annually</u> when required? Yes, annual SOC II Type 2

3.3.5. Status of System Security Plan (SSP)

In the table below, explicitly state whether the SSP is fully developed, partially developed, or non-existent. Identify any sections that the VENDOR has not yet developed.

Table 3-19. Maturity of the System Security Plan

Maturity of the System Security Plan
System security plan has been delivered during the transition in phase. Voyatek has analogous plans but this project involves hosting of a NC State provided system.

In the table below, state the number of controls identified as "Not applicable" in the SSP. List the Control Identifier for each, and indicate whether a justification for each has been provided in the SSP control statement.

Table 3-20. Controls Designated "Not Applicable"

<x> Controls are Designated "Not Applicable"

In the table below, state the number of controls with an alternative implementation. List the Control Identifier for each.

Table 3-21. Controls with an Alternative Implementation

<x> Controls have an Alternative Implementation

Organization's Security Representative or designee

PLEASE PRINT NAME

SIGNATURE

Date

d) Architecture Diagrams

The following diagrams were prepared using North Carolina's preferred format for architecture, technology stack, and data flow diagrams.

The network architecture diagram shows the components of the system architecture, such as virtual machines, networking components, and PaaS services, as deployed in an Azure cloud environment.

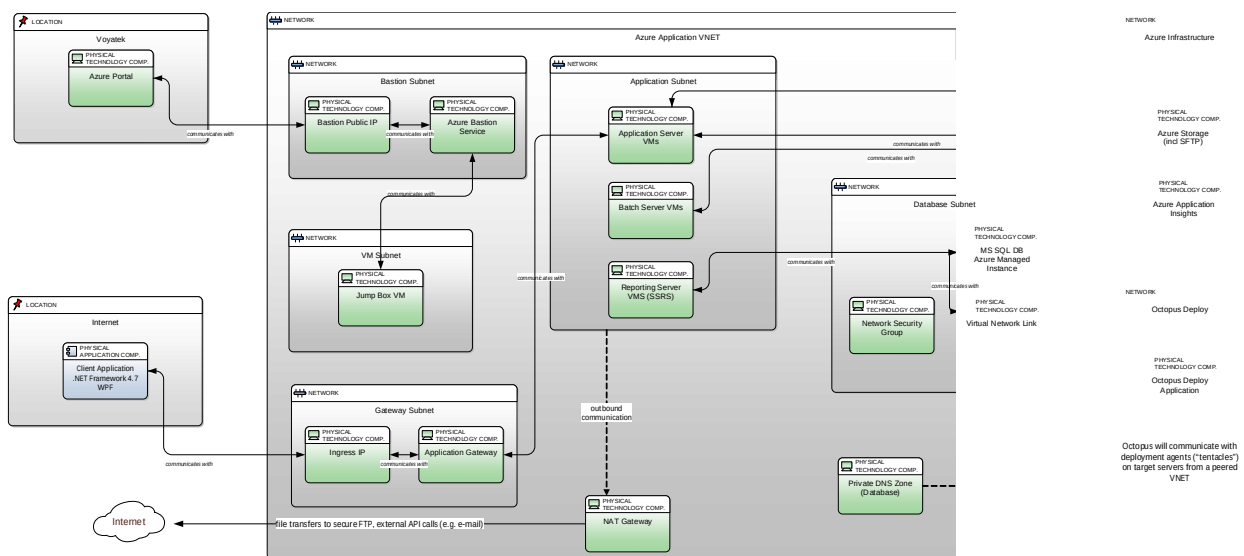


Figure 7: Crossroads Azure Network Architecture

The technology stack diagram shows the various technology components of the system and how they communicate with each other.

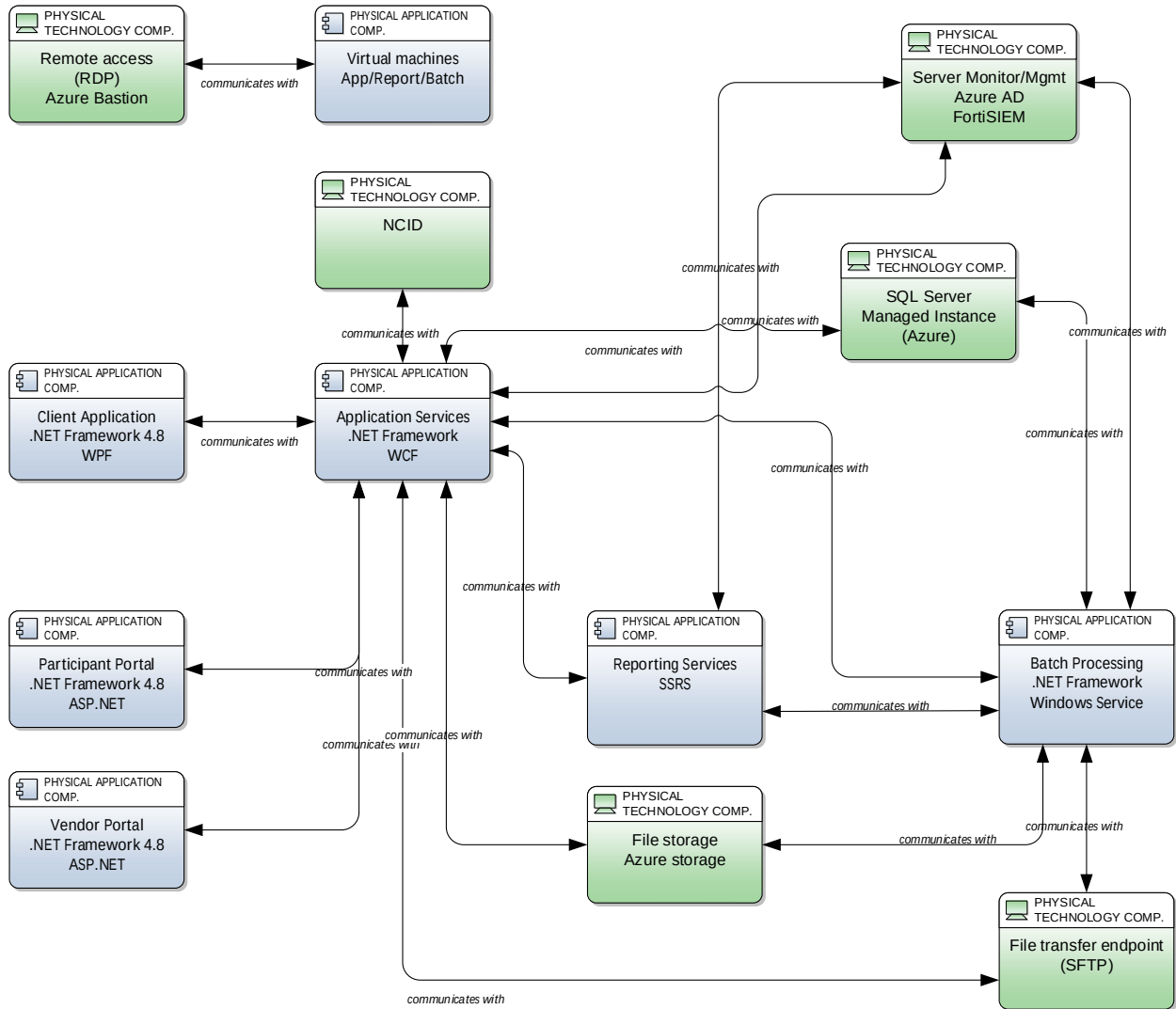


Figure 8: Technology Stack Diagram

The data communication diagram shows the types of data the system manages and what actors interact with the data.

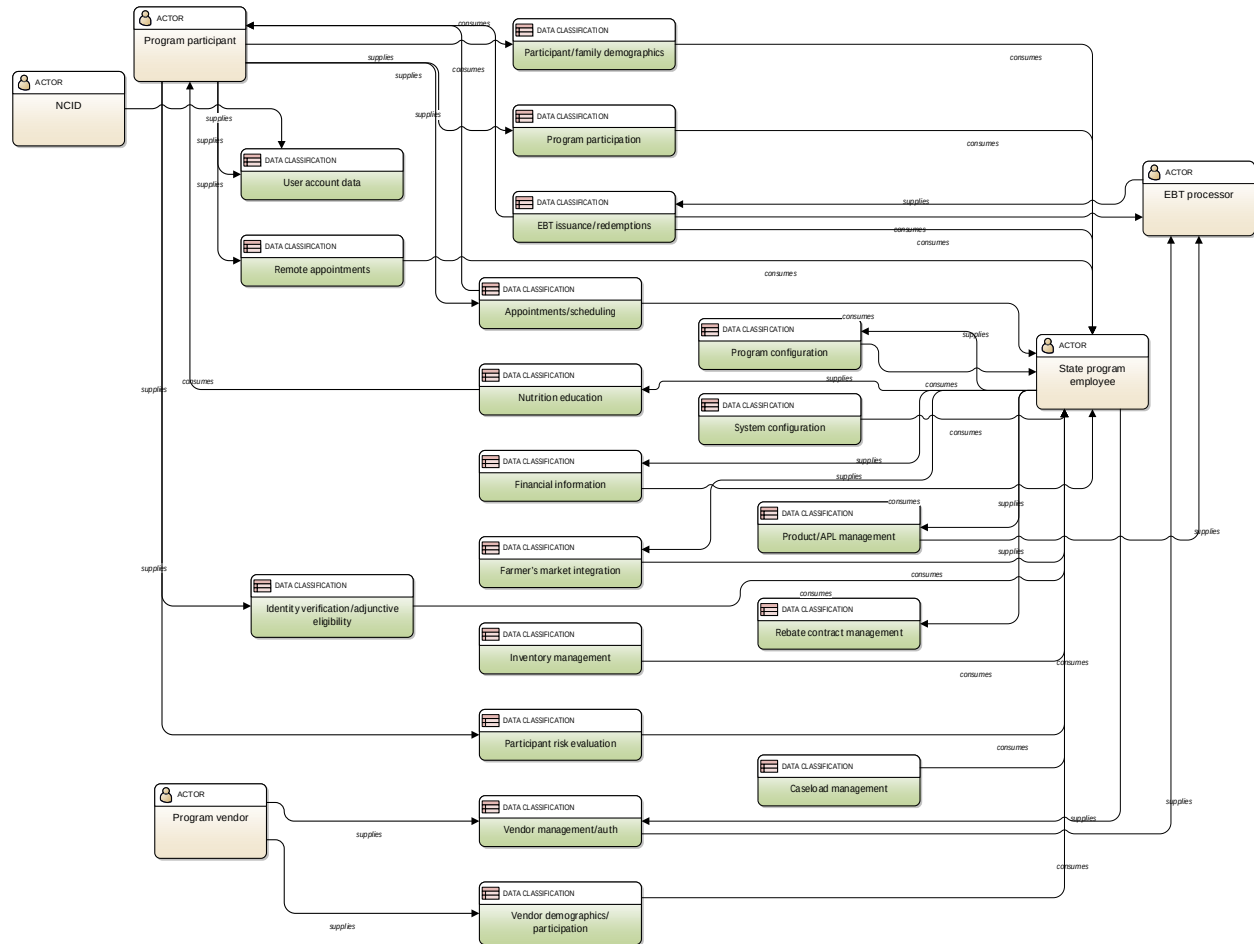


Figure 9: Data Communication Diagram

e) Detailed Project Timeline

Voyatek has prepared a proposed detailed timeline for the next Crossroads M&E Services contract. The timeline has been prepared as a Microsoft Project schedule with over 1000 individual tasks to properly capture the details throughout the contract duration. Many of these tasks are repetitive due to the cyclical nature of the ongoing M&E services. Voyatek has depicted this cyclical work as repeating lines on the timeline. The graphical representation of the timeline is shown on the next page in Figure 10.

The key elements of the services Voyatek will provide depicted in the timeline are:

- The contract starts August 1, 2025, as reflected in the RFP, with the Kickoff Meeting. The base period for the contract is seven years followed by up to three optional years, ending at maximum duration on July 31, 2035.
- The Transition-In Phase begins following the Kickoff Meeting and focuses on the rehosting of the system from the NC Data Center to the Azure Cloud. This is a 4-month effort.
- Also beginning after the Kickoff Meeting is the ongoing M&E for the Crossroads system. Due to the nature of the release planning for the first release to the cloud, some of this work must run in parallel with the Transition-In activities.
- Throughout the M&E Phase there are recurring activities that drive the release planning and delivery, including enhancements, as well as ongoing project management. The recurring tasks are:
 - o Weekly Status Meetings
 - o Monthly Status Reports
 - o Quarterly Schedule & Quality Reviews
 - o Monthly support activities for Crossroads Operations, Maintenance, & Hosting
 - o Regular system releases planned three times per year with a regular cadence for release design, development, UAT, and deployment
- At the end of the 7th year of the contract and at the end of each ensuing optional year is a possible Transition-Out period during which the Voyatek team may be turning over the responsibility for operating and hosting Crossroads to another entity.

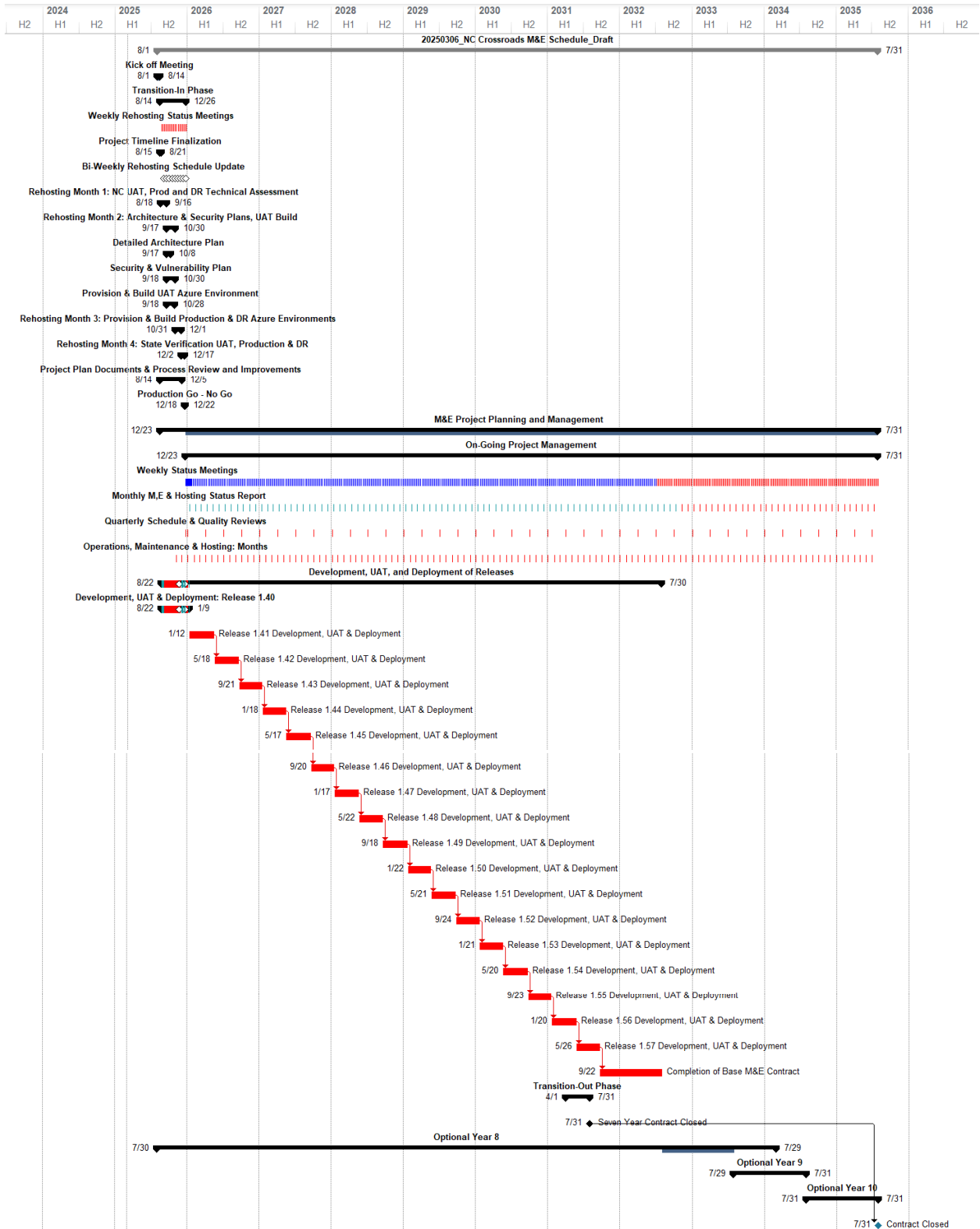


Figure 10: Detailed Project Timeline

f) Errata and Exceptions – Exceptions to Requirements and Specifications

Voyatek respectfully submits exceptions to a limited number of requirements and specifications and asks for the opportunity to discuss them with DHHS at the appropriate time. The intent of the exceptions is to maintain a cooperative, collaborative relationship between Voyatek and DHHS that focuses on delivering outcomes for DHHS.

Section	3.5.8.j) Time and Cost to Correct Defects
Page #	44
Exception	Voyatek takes exception to the requirement that all identified defects must be corrected before the System can be certified as ready for release deployment.
Explanation	Table 4 – Defect / Issue Classification Criteria defines five levels of defects. Among these are Minor and Trivial Issues. Examples of Trivial Issues include future enhancements and cosmetic changes. Requiring correction of all issues before the system can be certified as ready for release means that minor and trivial issues can become a blocker to a release that might fix more important functional issues and/or deliver enhancements to the system. Requiring correction of all issues also requires the allocation of resources to fix these minor and trivial issues instead of allowing personnel to begin work on items that are a higher priority and/or deliver more value to DHHS. Consequently, Voyatek asks that the System can be certified as ready for a release deployment if all priority level 1, 2, and 3 defects are corrected and priority level 4 (minor) and 5 (trivial) defects are placed into a backlog for a future release.

Section	3.5.12.j)
Page #	50-51
Exception	Voyatek takes exception DHHS' ability to defer acceptance of a Change Request until all required defect corrections have been implemented.
Explanation	The explanation is the same as for the exception to Section 3.5.8.j).

Section	Section 3.5.3.l) Service Level Agreement Table 3 – Service Level Agreement
Page #	32 - 33
Exception	The liquidated damages for the criteria are severe and there is no cap on the liquidated damages that can be applied each month.
Explanation	While liquidated damages are important for obtaining performance assurances from a contractor, they can reach a tipping point where the assessment of liquidated damages threatens contract performance. Large and uncapped

	liquidated damages, such as those found in Table 3, can create cash flow problems and strain a contractor's financial resources. The financial burden arising from the liquidated damages can reduce the contractor's capacity to manage unforeseen issues or invest in the contract. This can lead to further delays and further liquidated damages. Consequently, large, uncapped liquidated damages can create a vicious cycle where the contractor's ability to perform to the required standards is severely compromised, ultimately jeopardizing the overall success of the contract. Voyatek desires to negotiate a Service Level Agreement that provides performance assurances without threatening the success of the contract.

In addition to the exceptions to the RFP Requirements and Specifications in section 3 of the RFP, Voyatek wishes to discuss certain other sections of the RFP.

Section	Section 2: Terms and Conditions Applicable to Vendor Hosted Services 6) Performance Review and Accountability
Page #	86
Exception	Voyatek asks for the removal of the 10% retainage of each monthly Maintenance and Enhancement value in Attachment D plus 10% of each monthly Hosting value in Attachment D and withholding the final payment contingent on final acceptance by the State.
Explanation	Voyatek acknowledges that N.C.G.S. 143B-1340(f) requires contracts for information technology projects to include provisions for vendor performance and accountability. Voyatek also acknowledges that a retainage and withholding of final payments are permissible forms of performance assurance, as stated in 09 NCAC 06B.1207. However, Voyatek disagrees that retainage and withholding final payment are required or proper for this contract. First, 09 NCAC 06B.1207 authorizes multiple contract terms to meet the performance assurance required by statute. Liquidated damages (LDs) are among these contract terms authorized by 09 NCAC 06B.1207. This contract includes (LDs) (see Table 3 – Service Level Agreement). Voyatek agrees that Service Level Agreements (SLAs) and LDs are appropriate for this contract. Consequently, SLAs with LDs meet the statutory requirement. Therefore, retainage and withholding of final payment are not required. Second, while retainage and withholding a final payment are common performance assurances for an implementation contract, they are unusual for a maintenance and enhancements contract. SLAs with LDs are the most common form of performance assurance for a maintenance and enhancements contract. As explained above, this contract includes SLAs and LDs.

	Lastly, the vagueness in how DHHS would administer retainage and withholding final payment demonstrates that it is ill-suited to this maintenance and enhancement contract. Attachment D Cost Form has no “final payment” to be withheld. With the retainage, the conditions for release of the retainage are not defined. It is uncertain when, if ever, the retainage will be released. The possibility of retainage accumulating for up to 10 years is unacceptable for a maintenance and enhancement contract like this.

Section	Section 7.14 Special Terms and Conditions
Page #	67
Exception	Voyatek takes exception to a 5% liquidated damage on the Total Ten-Year Cost if any of the Transition-Out Period tasks or the Transition-Out Completion Report are not completed and accepted by the State by the Contract end date.
Explanation	Voyatek respectfully disagrees that the liquidated damage in Section 7.14 is a reasonable approximation of the damages that might be suffered by the State. For example, Section 3.5.14 includes a task for the contractor to provide 80 hours of technical training during Transition-Out. A contractor's shortfall in providing training hours would not cause hundreds of thousands of dollars of damage to the State. Voyatek asks to negotiate a liquidated damage rate that is not punitive.

g) Vendor's License and Maintenance Agreements

As required by the terms of this RFP, Voyatek will be responsible for maintaining the North Carolina owned Crossroads WIC MIS. Voyatek will provide hosting services using Microsoft Azure, Microsoft SQL Server, and other Microsoft licensed technologies that are currently required for the Crossroads WIC MIS. Voyatek and North Carolina will be subject to the licensing terms for the required products and services.

Voyatek does not propose any additional license or maintenance agreements outside of the final negotiated terms and conditions of this procurement. Voyatek accepts that the Crossroads WIC MIS is the property of North Carolina and that a temporary license to use the software on behalf of North Carolina WIC is being granted within this RFP.

h) Other Supporting Materials

Vendor may attach other supporting materials that it feels may improve the quality of its response. These materials should be included as items in a separate appendix.

Voyatek has added the following documentation as separate appendices:

- [Appendix Q: SOC 2](#)
- [Appendix R: Optional Services](#)

Appendices

Appendix A: Transition-In Plan

The following pages provide NC WIC the Transition-In Plan which describes the activities during the Transition-In Phase of the contract during which Voyatek will transition the hosting of Crossroads from the state data center to the Azure cloud.

State of North Carolina

Department of Health and Human Services

Division of Child and Family Well-Being



Crossroads MIS

Maintenance and Enhancement Services

North Carolina WIC Program

Appendix A

Transition-In Plan

Trademarks

Trademarked names may appear throughout this document. Rather than list the names and entities that own the trademarks or insert a trademark symbol with each mention of the trademarked name, the names are used only for editorial purposes and to the benefit of the trademark owner with no intention of infringing upon that trademark.

Contact Information

To request copies, suggest changes, or submit corrections, contact:

North Carolina Department of Health and Human Services**Division of Child and Family Well-being, WIC Program**

Attention: Molly Jones

Crossroads WIC Release Manager

Phone: 252-903-3951

Email: Molly.Jones@dhhs.nc.gov

Revision History

Date	Version	Revised By	Description
12/18/2018	0.1	Jay Saunders, Three Sigma Software	Draft version
3/6/2025	1.0	Jennifer Saunders, Voyatek	Submission for RFP 30-25002-DCFW

Deliverable Description

This Transition-In Plan describes the activities during the Transition-In Phase during which the driving activity will be the rehosting transition to Azure cloud managed by Voyatek and the fine tuning of project plans and processes to align with Voyatek assuming hosting responsibility for the Crossroads WIC system.

Table of Contents

1	Introduction	1
2	Transition Communications.....	2
2.1	Kickoff Meeting.....	2
2.2	Crossroads Transition Overview.....	2
2.3	Technical Coordination Sessions	2
2.4	Change Request and Release Planning	3
2.5	First Release.....	3
3	Phase Documentation Deliverables	4
3.1	Product Work Plan and Schedule.....	4
3.2	Maintenance and Enhancement Status Reports.....	4
3.3	UAT Deployments	4
3.4	Final Release Notes and System Documentation.....	4
3.5	Production Deployment Plan.....	4
3.6	Risk and Security Assessment of Vendor Critical Systems and Infrastructure	5
3.7	Other Deliverables	5
4	Staffing and Training.....	6
4.1	Staff Recruitment.....	6
4.2	Training.....	6
4.3	Access Requests and NCID Credentials	6
4.4	NDA Signatures	6
5	Transfer of Materials	7
5.1	State Owned Hardware	7
5.2	Source Code & History.....	7
5.3	Issue Log.....	7
5.4	Project Documentation.....	7
6	Rehosting of NC Crossroads MIS	8
6.1	High-level Rehosting Schedule	8

1 Introduction

Voyatek anticipates a smooth a transition-in as we continue as the Maintenance and Enhancement provider and we anticipate that not all the typical transition-in activities will be necessary. Our primary objective during the Transition-In Phase will be to complete the rehosting of the NC Crossroads system and to assume responsibility for NC Crossroads hosting and maintenance, and updating project plans and processes to align with these new responsibilities.

Based on the clarifications provided through the RFP process, Voyatek's understanding is that all M&E support for the system running in the NC Data Center will be provided by Voyatek under our current contract. Upon execution of the new contract, we will begin the preparation for transitioning the system to the Azure cloud platform. These transition activities are described in **Error! Reference source not found..** The transition will be completed during the 8-month Transition-In period. Upon cutover of the production Crossroads system to the Azure cloud, the Voyatek team will:

- Continue support of NC Crossroads with the M&E costs covered under our current contract.
- Commence hosting support for the new cloud platform under the new contract.
- Support the NC Data Center team as needed to complete the decommissioning of the data center platform as the final portion of the current contract.
- At the end of the Transition-In Phase, as the current contract ends, our team will commence M&E services under the new contract for the Crossroads WIC MIS rehosted in the cloud.

2 Transition Communications

2.1 Kickoff Meeting

The Voyatek Product Manager will coordinate with the Crossroads WIC Release Manager and DPH management to schedule a Kick-Off Meeting to review the scope, deliverables, and schedule for the new contract and to identify key differences from the current M&E contract so that parties and stakeholders are clear on how the transition to the new contract will work. To facilitate the four (4) month rehosting schedule in our proposal, Voyatek prefers to hold the Kickoff meeting as soon as possible. It is an important opportunity to review key project tasks and timeline with North Carolina WIC staff, NC DIT and other stakeholders. The Voyatek Product Manager will work with the Crossroads WIC Release Manager to build the agenda and develop written materials prior to the kickoff meeting.

There will be two concurrent streams of activity to review during the meeting:

- Rehosting of NC Crossroads
- Reviewing and updating M&E plans to align with Voyatek hosting and the final contract

We recognize the importance and effectiveness of in-person meetings, however, Voyatek would like to offer the option to hold the Kickoff Meeting via conference call and to reserve the onsite meeting to occur further in the Transition-In Phase, such as for technical coordination of rehosting activities. Voyatek will send at least 3 representatives to provide support at the onsite meeting, whether for the Kickoff meeting or for a meeting later in Transition-In.

After the Kickoff meeting, the Voyatek Product Manager will summarize the decisions, issues, and action items from the meeting in a memorandum and submit it to the State for review and approval.

2.2 Crossroads Transition Overview

This Transition-In Plan as well as the *Appendix E-Rehosting Implementation and Rollout Plan*, and *Appendix C-Product Work Plan and Schedule* are the most relevant documents for the Transition-In Phase. Voyatek will walk through these documents with North Carolina staff shortly after Kickoff.

2.3 Technical Coordination Sessions

Through a series of meetings during Month 1 of Transition-In, Voyatek will work closely with NC DIT to review and document the current Crossroads environments' infrastructure, configurations, dependencies, and constraints that may impact the transition. The Voyatek Product Manager and the Crossroads WIC Release Manager will work together to coordinate these initial sessions to start shortly after the Kickoff meeting. Additional technical meetings will be coordinated through a weekly Rehosting Status call.

The Voyatek M&E team will continue to need access to the current environments through the transition. As the new environments are built and made available, both the Voyatek M&E and NC WIC staff access will be created. Reviewing existing support procedures and establishing new support procedures will be completed by Voyatek, NC WIC and NC technical staff so that all persons supporting the project have the information needed for the new environments.

2.4 Change Request and Release Planning

Voyatek anticipates that planning for the first release in the new Maintenance and Enhancement Contract will occur during the Transition-In period. Voyatek will continue the cadence of quarterly planning meetings to review change requests with one annual on-site meeting in Raleigh, NC. The quarterly meetings will include review of change requests and business needs, Joint Application Design sessions, and coordination and release planning with North Carolina staff.

Voyatek believes that working directly with customers when reviewing software features and needs greatly improves the ability to design and deliver quality solutions. Voyatek understands that the scope of the first scheduled release will be limited but our team would like the opportunity to schedule the first remote release planning meeting during Transition-In to begin the process and review the objectives of the first release.

2.5 First Release

Voyatek's Production Deployment Plan will take into consideration the release-in-progress at the time of Kickoff; however, Voyatek M&E staff will begin analysis and development on changes prior to the transition to cloud hosting. The team would complete development and testing of the changes within the new cloud environments. Our resource plan allows for a minimum of 200 hours of change orders and 20 defect corrections (or less as determined by NC WIC) to be included in the first release to Azure.

Voyatek is committed to being fully operational in the cloud by the start of the Maintenance and Enhancement phase of the project.

3 Phase Documentation Deliverables

3.1 Product Work Plan and Schedule

The draft Product Work Plan and Schedule was delivered with our RFP response. One of the first activities will be to walk through the work plan and schedule in coordination with the Crossroads WIC Release Manager and deliver the final version for approval within 45 days of contract execution.

3.2 Maintenance and Enhancement Status Reports

Voyatek anticipates continuing with the current cadence for delivering the monthly Status Report by the 10th of each month. During Transition-In the Voyatek Product Manager will work with the Crossroads WIC Release Manager to determine if any adjustments to the report template or delivery timeframe are necessitated by the new contract, such as adding the Maintenance and Hosting status to this report or create a separate status report. As appropriate, the Voyatek Product Manager will revise the template and deliver to the Crossroads WIC Release Manager. The revised template will be used from the following month onward.

3.3 UAT Deployments

As part of the weekly NC Project Status meeting, Voyatek will provide updates on the status of the release in-progress such as but not limited to the UAT deployment timeline. Voyatek, when appropriate will provide testing guidance, meet with NC testers to discuss data setup, and review questions NC testers may have when preparing for and during UAT activities. Voyatek will work with the Crossroads WIC Release Manager to coordinate UAT deployments to minimize impact to staff who may be using UAT for other activities. The Crossroads WIC Release Manager will notify NC staff of UAT deployment dates and times. Voyatek will provide release notes with each deployment to UAT.

3.4 Final Release Notes and System Documentation

Voyatek will provide the final version of the Release Notes at completion of UAT activities documenting the final and confirmed release content that will be deployed to production. Delivery of system documentation updates will be coordinated with NC. Currently documentation is delivered to a secure FTP site and maintained in the North Carolina SharePoint site.

3.5 Production Deployment Plan

Since Voyatek took over M&E services, the NC Crossroads Release Manager created and maintained the Production Deployment Plan to facilitate coordination of resources and timelines for each step of the deployment as assigned to Voyatek, NC WIC, and NC DIT staff. When Crossroads is transitioned to cloud, the complexity of coordination will be reduced considerably. As part of preparation for the first release deployment to Azure, the Voyatek Product Manager will work with the Crossroads WIC Release Manager to build the Production Deployment Plan template. Going forward, the Voyatek Product Manager will take over responsibility for the deployment plan with the support of the Crossroads WIC Release Manager who will coordinate the participation of all NC resources as appropriate.

3.6 Risk and Security Assessment of Vendor Critical Systems and Infrastructure

As part of the transition-in process, Voyatek will provide an updated security and vulnerability plan that provides a cross-reference between NC State security controls and requirements to Voyatek's internal policies and procedures along with related SOC 2 controls. Additionally, we anticipate that the most recent SOC2 report will be delivered prior to contract start if not at contract start.

3.7 Other Deliverables

Voyatek assumes that feedback may be provided on plans submitted with this proposal. If feedback is provided following contract award or during project review sessions, documents will be updated and saved to the NC Crossroads SharePoint site hosted by Voyatek. All plans will be updated to reflect non-draft versions and to baseline document versioning at 1.0.

4 Staffing and Training

4.1 Staff Recruitment

Proposed staff to support the Crossroads M&E contract are current staff and will continue to support the North Carolina Maintenance and Enhancement project from the start of the Transition-In phase. Since the original contract, Voyatek has expanded our Crossroads customers to include the four Crossroads User Group states and the State of Washington WIC program. With our growing customer base, we are working to expand our Crossroads technical resources. With a growing Crossroads Practice, we will continue to leverage our Crossroads experience to support North Carolina as needed.

4.2 Training

As new resources join the NC Crossroads team, whether permanent or for temporary assignment, Voyatek project staff will perform internal training led by business analysis, quality assurance, and development. For staff new to WIC, the Voyatek Project Director provides a general overview WIC and specific aspects of the NC WIC program, and the NC Crossroads project.

4.3 Access Requests and NCID Credentials

At Kickoff, Voyatek will confirm the list of team members whose access and NCID credentials should remain active and also provide the list of any new team members being added to the project and who will need access to State environments. If a team member leaves the NC Crossroads project, the Voyatek Product Manager will notify the Crossroads WIC Release Manager and the NC DIT contact as soon as possible. Throughout the project, Voyatek Product Manager will continue to comply with NC's DIT process to confirm user accounts and access on a quarterly basis.

4.4 NDA Signatures

If NC requires that Voyatek team members who currently have access to Crossroads Confidential Information to resubmit a signed Non-Disclosure agreements as part of the new contract, we will submit these within 15 calendar days of contract award. As additional team members are identified as needing access, these staff will complete the form and the Voyatek Product Manager will submit to NC DIT and the Crossroads WIC Release Manager.

5 Transfer of Materials

As the vendor for the current Crossroads M&E project, no materials need to be transferred to Voyatek to continue support under the new contract. Therefore, this section is referencing materials that continue to apply under the new contract.

5.1 State Owned Hardware

During the original contract, Voyatek received state owned equipment from the previous vendor. This equipment has been useful in providing quality assurance and help desk support, especially signature pads and POS devices. We will include the North Carolina equipment that has been transferred to Voyatek under the previous contract in this review.

This list of hardware includes:

- Document scanner/printer
- Card Readers
- Signature Pads
- Anthropometric hardware in use by North Carolina
- POS Stand beside device (for redemption testing with CDP)

Voyatek maintains a large library of WIC related hardware. Some items like stand beside point of sale devices are only applicable if there is a testing mechanism with the current EBT vendor.

5.2 Source Code & History

Voyatek maintains the NC Crossroads source code library including change history. Under the original contract, Voyatek uploads the source code for each release to a secure FTP site that NC has access to. For the last release delivered under the previous contract, Voyatek will transfer the release source code library to the state via this existing SFTP site. Once the cloud transition has been completed, Voyatek will work with the state to discuss optional methods for delivering source code to the state for releases deployed in Azure.

5.3 Issue Log

Voyatek maintains the current Crossroads Issue Log in Azure DevOps. Refer to Appendix J – Configuration Management and Release Management Plan for more information on Azure DevOps. This will continue to be our issue tracking tool. The Voyatek Product Manager and Crossroads WIC Release Manager will confirm the NC staff who need access and update as appropriate.

5.4 Project Documentation

The initial documentation delivered to Voyatek under the original contract included an extensive documentation library including DFDD's, risk code documentation, user manuals, DTS and white papers, data dictionaries, ICDs, ECDs, RDDs, installation and configuration guides, and the CPS Operations Manual. This documentation is stored in Voyatek's North Carolina SharePoint site. Additionally, documentation updates made by Voyatek team members are also maintained in this SharePoint site. Documentation updates provided for each release are also delivered to the SFTP site and or email. The SharePoint site will continue to be the documentation repository. The Voyatek Product Manager and Crossroads WIC Release Manager will confirm the NC staff who need access and update as appropriate.

6 Rehosting of NC Crossroads MIS

A major part of the Transition-In Phase is moving Crossroads to cloud hosting. Voyatek has long experience with maintaining the system in North Carolina. We were proud to have successfully completed the last transition in 2019 during which the foundation for this current transition was built. In that transition and during the course of the first year of support:

- Crossroads source code build processes were formalized and automated in Azure DevOps
- Both vendor and state environment deployment processes were completely automated using Octopus Deploy
- The release cadence for the Crossroads system was increased so new features and bug fixes could be released to users promptly

In the years since, our automated deployment processes have enabled accurate and efficient system release updates with much less effort and without manual effort, a more reliable and stable approach. Moving the Crossroads system to the cloud dovetails well with our approach for automating build and deployment processes for both software and hosting environments.

Appendix E - Rehosting Implementation and Rollout Plan outlines the strategy and technical approach for migrating the Crossroads environments that are currently located in an on-premises North Carolina datacenter to a Voyatek managed Azure tenant. The plan will address the migration of the following environments.

1. UAT
2. Staging
3. Sandbox
4. Production
5. Disaster Recovery

Following successful migration of the UAT environment, the production transition will be scheduled and will utilize the procedures verified in the UAT migration. Voyatek anticipates being able to complete the production migration during a weekend with little or no impact to clinic operations.

6.1 High-level Rehosting Schedule

- **Month 1**
 - o Voyatek and NC DIT conduct a series of meetings to review existing infrastructure, capture detailed configurations, and identify any discrepancies or constraints that may impact transition, and
 - o Voyatek updates the Detailed Migration Task Schedule.
- **Month 2**
 - o Voyatek begins development of a detailed architecture plan and updates to the hosting security plan for the target environment outlining the proposed infrastructure, security controls, scalability considerations, and compliance with relevant standards and policies.
 - o Voyatek begins building the UAT Azure environment, and
 - o Voyatek updates the Detailed Migration Task Schedule
- **Month 3**
 - o Voyatek submits the architecture plan and hosting security plan

- o Voyatek collaborates with NC DIT to address any concerns, incorporate feedback, and refine the plans to align with operational and security requirements
 - o Voyatek completes testing and verification of UAT
 - o Voyatek seeks final approval of the architecture and security plans
 - o Upon final approval, Voyatek provisions the Production and DR environments
 - o Voyatek updates the Detailed Migration Task Schedule
- **Month 4**
 - o State initiates verification by conducting a comprehensive review and validation of the newly provisioned environments
 - o Voyatek will finalize and update any infrastructure-related project documentation to reflect the end-state system
 - o Voyatek and WIC complete final readiness assessments and go-live planning, including coordination with WIC and NCDIT stakeholders to designate a final cutover date
 - o NC WIC provides approval for cut over
 - o Voyatek, WIC and NCDIT complete Production cut over to Azure
 - o NC Crossroad production is live in Azure

Appendix B: Product Management Plan

The following pages provide NC WIC with the Product Management Plan which describes Voyatek's approach to managing the North Carolina Crossroads Maintenance and Enhancement project. The Product Management Plan is the overarching "umbrella" Plan that defines how the contract is executed, monitored, controlled, and closed.

State of North Carolina

Department of Health and Human Services

Division of Child and Family Well-Being



Crossroads MIS

Maintenance and Enhancement Services

North Carolina WIC Program

Appendix B

Product Management Plan

Trademarks

Trademarked names may appear throughout this document. Rather than list the names and entities that own the trademarks or insert a trademark symbol with each mention of the trademarked name, the names are used only for editorial purposes and to the benefit of the trademark owner with no intention of infringing upon that trademark.

Contact Information

To request copies, suggest changes, or submit corrections, contact:

North Carolina Department of Health and Human Services**Division of Child and Family Well-being, WIC Program**

Attention: Molly Jones

Crossroads WIC Release Manager

Phone: 252-903-3951

Email: Molly.Jones@dhhs.nc.gov

Revision History

Date	Version	Revised By	Description
12/18/2018	0.1	Jay Saunders, Three Sigma Software	Draft version
3/6/2025	1.0	Jennifer Saunders, Voyatek	Submission for RFP 30-25002-DCFW

Deliverable Description

This Product Management Plan describes Voyatek’s approach to managing the North Carolina Crossroads Maintenance and Enhancement project. The Product Management Plan is the overarching “umbrella” Plan that defines how the contract is executed, monitored, controlled, and closed.

Table of Contents

1. Introduction	1
1.1 Business Need/Problem	1
1.2 Project Objectives	2
1.3 Roles and Responsibilities	2
1.4 Product Governance	7
1.5 Status Reporting.....	8
2. Scope Management Plan.....	9
2.1 Project Scope Statement.....	9
2.2 Exclusions.....	12
2.3 Assumptions	12
2.4 Project Facilities Location	13
3. Schedule Management Plan	14
3.1 Roles and Responsibilities for Schedule Development	14
3.2 Schedule Control and Reporting.....	15
3.3 Schedule Changes and Thresholds	15
4. Staffing Management Plan.....	16
4.1 Roles and Responsibilities	16
4.2 Responsibility and Assignments	19
4.3 Acquisition Strategy	23
4.4 Organization Chart.....	23
5. Product Work Plan and Schedule	25
6. Quality Management.....	26
7. Communications Management.....	27
8. Risk and Issues Management	28
9. Collaboration Web Site	29
9.1 Documents, Deliverables, and Records Management	29
9.2 Action Item Tracking Tool	29
10. Change Management	30
10.1 System Change Request Process	30
10.2 CR Initiation, CR Validation, and Initial Response.....	31
10.3 Authorize Detailed Analysis and CR Authorization	32
10.4 CR Deployment	32

10.5	Changes to Reference Tables	32
10.6	Changes Outside the Scope of the RFP	33
10.7	Corrections / Defect Fixes to Correct Deficiencies	33
10.8	Document Updates	34
10.9	Document Update Process	34
10.10	Process to Log and Track pending CRs	34
11.	System Design and Development Management	35
11.1	NC Technical Architecture System Design (TASD).....	35
11.2	Capacity Management	35
11.3	System Documentation	36
12.	Test Management	37
13.	Configuration and Release Management	38
14.	Security and Vulnerability Management	39
15.	Training Management.....	40
16.	Disaster Recovery and Contingency Plan.....	41
17.	Partnerships and Contractual Relationships Plan	42
18.	Help Desk Support.....	43
19.	Transition-In Management.....	44
20.	Transition-Out Management	45

Table of Figures

Figure 1: North Carolina Crossroads MIS Product Team Organization Chart	24

Table of Tables

Table 1: Product Management Plan Topics.....	1
Table 2: Voyatek Roles and Responsibilities for the Crossroads Product	2
Table 3: Additional Staff Supporting Crossroads	6
Table 4: List of Product Deliverables.....	10
Table 5: RACI matrix for the North Carolina Crossroads Maintenance & Enhancement project	21
Table 6: Change Request Process – Roles and Responsibilities	30
Table 7: Defect Priority Classification	33

1. Introduction

The objective of this document is to describe the efforts and tasks associated with the Voyatek responsibilities within the North Carolina Crossroads Maintenance and Enhancement project. This plan includes the purpose, scope, goals, and objectives of the project. This plan also addresses project management topics such as communication plans and risk management plans. Some of these topics will be fully covered in a companion document and will be only referenced here in this master Product Management Plan.

Content in this plan include the following topics:

Table 1: Product Management Plan Topics

• Scope Management	• Test Management
• Schedule Management	• Security and Vulnerability Management
• Quality Management	• Disaster Recovery
• Staffing Management	• Help Desk Support
• Communications Management	• Action Item Tracking Tool
• Risk and Issues Management	• Release Management
• System Design and Development Management	• Documents, Deliverables, and Records Management
• Capacity Management	• Collaboration Web Site
• Status Reporting	• Transition-In Management
• Change Management	• NC Technical Architecture System Design (TASD)
• Product Governance	• Software Build Tools
• Training Management	• Transition-Out Management
• Scope Management	• Test Management
• Schedule Management	• Security and Vulnerability Management

1.1 Business Need/Problem

The State of North Carolina utilizes the Crossroads Management Information System to support its Supplemental Nutrition Program for Women, Infants, and Children (WIC) program in delivering nutritional services to low-income pregnant, postpartum and breastfeeding women, infants, and children up to age five who are at nutritional risk. The Crossroads Consortium was created in 2005 in response to the FNS State Agency Model (SAM) mandate for designing, building, and implementing new WIC management information systems (MIS) nationwide. The Crossroads Consortium, with North Carolina as the lead state, awarded a contract to the incumbent vendor Computer Sciences Corporation (CSC) in 2009 to build a SAM system for the states of Alabama, North Carolina, Virginia, and West Virginia. Rollout of the Crossroads SAM system was completed in all four (4) Crossroads Consortium states by 2014, with the North Carolina instance of Crossroads being hosted by the NC Department of Information Technology. In 2017, North Carolina amended the Crossroads contract with CSC to continue providing Maintenance and Enhancement Services using source code and documentation independent of the other three Consortium states. In 2019, North Carolina awarded their next Maintenance and Enhancement Services contract to Voyatek to provide services including

defect correction, change order implementation, software installation services, and production help desk support.

The Crossroads Maintenance and Enhancement Project is to provide maintenance and enhancement services of the North Carolina Crossroads WIC Management Information System described in Section 2 of the NC Crossroads M&E RFP 30-25002-DCFV document beginning on August 1, 2025.

1.2 Project Objectives

The primary project objectives include:

- a) Transition-in and Transition-out
- b) Perform maintenance to the WIC Crossroads application. Maintenance also includes the following items:
 - i. Defect correction
 - ii. Change order implementation
 - iii. Software installation services, and
 - iv. Production help desk support
- c) Perform enhancements to the WIC Crossroads application

1.3 Roles and Responsibilities

To transition support of the Crossroads product and to deliver maintenance and enhancement services, the following roles and responsibilities have been identified and assigned for completion of tasks. Those listed in Table 1 will be the lead resources for the associated responsibilities.

Refer to the **Staffing Management Plan** section for more information regarding Voyatek’s staffing for this project.

Table 2: Voyatek Roles and Responsibilities for the Crossroads Product

Role	Responsibilities
Voyatek Product Manager (Key Staff) Jennifer Saunders	Responsible for overall project execution, accomplishment of all project deliverables, the daily work of M&E Contractor personnel, and coordination of work with North Carolina WIC staff. Responsibilities include: • Serve as the primary point of contact for the contract and project for North Carolina WIC and other NC entities • Provide both contract administration and project management throughout the contract • Coordinate Voyatek resources for execution of the WIC MIS project with full authority to commit Voyatek on matters concerning the contract

Role	Responsibilities
	• Ensure that all project deliverables and services are provided on time, within scope and within budget • Develop project plans and objectives, involving all relevant stakeholders and ensuring technical feasibility • Ensure resource availability and allocation • Develop a detailed project plan to track progress • Use appropriate verification techniques to manage changes in project scope, schedule and costs • Measure project performance using appropriate systems, tools and techniques • Report and escalate to management as needed • Manage the relationship with North Carolina WIC and all stakeholders • Perform risk management to minimize project risks • Establish and maintain relationships with third parties/vendors when needed • Create and maintain comprehensive project management documentation • Notify the DHHS Release Manager, verbally within one business hour and in writing within one business day, when Voyatek discovers any problem(s) that may jeopardize the successful or timely completion of our contract obligations
Voyatek Business Analyst Manager (Key Staff) Cindy Kochersperger	Leads the team of Business Analysts who will assist in defining the business and functional requirements. Responsibilities include: • Manage the overall requirements and requirements verification process

Role	Responsibilities
	• Lead and create change requests responses and estimates • Provide daily technical guidance for the business analysts • Work with well-established processes in a team environment • Ensure that workflow in the system is optimized • Ensure that customer requirements are accurately reflected in the system and in system documentation • Validate that test scripts fully satisfy North Carolina’s business requirements and needs • Support the North Carolina Help Desk, including assisting with data corrections
Voyatek Development Manager (Key Staff) Michael Heinrich	Leads the team of developers who will configure the platform to meet the business requirements. Responsibilities include: • Manage the software build baseline, including management of system configuration and architecture changes • Provide daily technical guidance for the development team • Develop necessary user interface software to meet requirements, including maintaining and enhancing the critical interface to the EBT system. • Develop necessary system interface software to meet requirements • Develop necessary software/scripts to manage database layer • Develop necessary software to manage business operations layer • Ensure the optimal application of technology and engineering resources to meet customer requirements

Role	Responsibilities
	• Maintain and support the system design for approved enhancements
Voyatek Test Manager (Key Staff) Helena Young	Manages the testing efforts, including end to end system testing, regression testing, and performance testing. Responsibilities include: • Manage the overall end-to-end system testing processes during maintenance and enhancement phases inclusive of User Acceptance Testing (UAT) • Maintain and manage well-established test processes in a team environment • Test highly complex code and integrated system capabilities • Ensure that the system functions correctly across different environments • Conduct tests to verify user functionality and system configuration • Investigate and resolve matters of significance for end-user problems • Write test scripts, test reports, requirement documents and other related technical documents • Produce test reports to summarize all testing activities for clients
Voyatek Advisory Technical Architect Jon Moreau	Responsible for the technical architecture and ensuring that a solution is implemented to meet all system and security requirements. Responsibilities include: • Providing technical direction and guidance, as well as hands-on project management, for all product and software development • Ensuring the optimal application of technology and engineering resources to meet customer requirements • Ensuring that the product is fully and correctly defined and documented

Role	Responsibilities
	Ensuring implementation of formal processes to support the product
Voyatek JAD and Training Support Cindy Kochersperger	Responsible for supporting the development of new enhancements by leading JAD sessions and the subsequent training efforts, as requested by NC. Responsibilities include: - Leading the design sessions to develop and verify requirements for enhancements to the Crossroads system - Leading the development of appropriate training material when required for enhancements

In addition to the above named lead staff, Voyatek will assign additional staff to the following roles to support Crossroads Release development and Product support on an as needed basis when such skillsets are needed to deliver services or when change requests to enhance the product warrants additional staffing.

Table 3: Additional Staff Supporting Crossroads

Role	Responsibilities
Voyatek Developers	Provide the required work to refine business processes to ensure all requirements are met. Responsibilities include: - Develop necessary user interface software to meet requirements - Develop necessary system interface software to meet requirements - Develop necessary software/scripts to manage database layer - Develop necessary software to manage business operations layer
Voyatek Business Analysts	Provide the required work to refine business processes to ensure all requirements are met. Responsibilities include: - Work with well-established processes in a team environment - Ensure that workflow in the system is optimized

Role	Responsibilities
	• Ensure that customer requirements are accurately reflected in the system and in system documentation
Voyatek Testers	Provide the required software testing to ensure all requirements are met. Responsibilities include: • Work with well-established processes in a team environment • Test highly complex code and integrated capabilities • Ensure that web pages are functional across different environments • Conduct tests to verify user functionality • Investigate and resolve matters of significance for end-user problems and escalate if necessary • Write test scripts, requirement documents and other related technical documents
Voyatek Training Teams	Provide the required training to ensure all requirements are met. Responsibilities include: • Organize and develop, or obtain, training procedure manuals and guides and course materials such as handouts and visual materials • Assess training needs through surveys, interviews with employees, focus groups, or consultation with managers, instructors or customer representatives

1.4 Product Governance

Voyatek and the North Carolina Department of Health and Human Services are jointly responsible for managing the project and committing the necessary effort and resources to support their respective staff to fulfill their contractual obligations. As such, both organizations have identified a single point of contact to make sure that management and oversight are sufficient to complete project tasks. The Voyatek Product Manager will be point of contact for Voyatek and will report directly to the Voyatek Executive Committee regarding project activities. The Crossroads WIC MIS Release Manager serves as the primary point of contact for the State.

Our mission is to provide our customers with quality software development, implementation, and maintenance support to effectively manage their Women, Infants, and Children (WIC) programs. Voyatek approaches each project as a partnership with our customers to deliver quality services to WIC staff and by extension, helping the WIC program to provide efficient and effective services to their participants. Our approach to project management is to encourage:

- Open communication and participation so that project team members, stakeholders and project sponsors are well informed and engaged
- Responsiveness and flexibility to support stakeholders and team members in a timely manner with the ability to make changes as business needs change
- Effectiveness and efficiency in processes and actions to make the best use of resources and time available to the project

This Product Management Plan, with the Contract and the subordinate plans and processes, provides the structure within which project team members will manage and perform their tasks. Throughout the duration of the project, it is anticipated that these plans and processes will mature and develop, thus improving our partnership with North Carolina and our support of the WIC program.

1.5 Status Reporting

Voyatek will provide monthly project status reports, throughout all phases of the project, in a format that is agreeable to North Carolina. A review of the current content of project status reports will be conducted with the State during Transition-In to confirm any changes to the status report format. The status report will be used to track progress against the Work Plan. Voyatek includes the following information in our standard status report format; however, we will tailor the report to the State's needs.

The Voyatek template includes the project name, reporting period, and the name of the staff person completing the report. In addition to a Project Status summary of activities that have occurred during the reporting period, the following information will be included in the report:

- Work tasks completed during the prior month
- BA, Development and QA Team tasks completed during the month
- Open Issues
- Production Issues
- Release-in-progress content list with Azure DevOps ID, work item type, state, priority, etc.
- Release-in-planning content list, as appropriate
- Risk Tracking Log
- Service Level Agreement
- Open Change Requests

Updates to the Project Schedule and WBS will be documented in the Status Report as needed. Topics specific to each phase or unique activities may be added, as well.

2. Scope Management Plan

North Carolina Crossroads RFP identifies the overarching scope for the project. Voyatek's response provides further definition of project scope and the activities and processes we will utilize to perform under the contract. While these documents provide the definition of the work to be performed, further definition of scope will be a natural part of the project so that staff may successfully perform their tasks. Thus, scope management will be an ongoing task of the Voyatek Product Manager and the Crossroads WIC MIS Release Manager to define, validate and manage activities to prevent scope creep.

Several processes and plans will aid us in managing and controlling scope changes for this project. As noted above, the contract defines the overall project scope. This Product Management Plan defines the overall management of the project, and the subordinate plans provide more definition for the specific areas requiring formal management of the work to be performed. While all plans and processes facilitate managing the overall delivery of services and goods within the scope of the contract, certain plans and processes are key to managing and controlling scope. The key plans and processes for managing scope are the Product Work Plan, the Schedule Management Plan, System Change Request Process, requirements definition and documentation, the Quality Assurance Management Plan, Risk and Issues Management, and the Communication and Coordination Plan.

All team members, Voyatek and DHHS staff, should be familiar with these plans and processes to be able to identify potential change in scope and bring it to the attention of the Voyatek Product Manager and the Crossroads WIC MIS Release Manager such that they can assess the change, validate whether it is within scope, and manage activities to properly execute a change order or to bring activities within the defined scope.

Any changes deemed out of scope will be managed through Change Management and System Change. Those change requests that have been approved by North Carolina will be evaluated by Voyatek for the effect of the scope change on the current schedule and budget. The impact analysis will be reviewed with North Carolina to determine if a change order is necessary. If the scope change will significantly affect the current project schedule, the Voyatek Product Manager may request that the schedule be re-baselined in consideration of the new project scope. North Carolina must review and approve change requests before the schedule can be re-baselined.

2.1 Project Scope Statement

The Crossroads Maintenance and Enhancement project will have two phases: Transition-In phase and Maintenance and Enhancement phase. The Transition-In phase will start right after contract execution and the primary focus will be the transition of hosting responsibility for Crossroads from the DHHS to Voyatek's cloud solution. This Transition-In phase will include:

- Project kickoff with North Carolina
- Review of the proposed hosting solution (either virtual or in person) with NC WIC and Department of Information Technology to finalize the hosting solution and related services
- Discuss and build the schedule and plan for the hosting transition
- Submit request for any needed State-owned hardware for consideration by the State for approval
- Review of Document Deliverables noted in Table 1 delivered with Voyatek's proposal
- Confirmation of product documentation and artifacts including DFDD and Risk Code documentation, User Manuals, DTS and White Papers, Data Dictionary, ICD, ECD, RDD,

Installation and Configuration Instructions, and the CPS Operations Manual, and regression and performance test artifacts

- Initiation of the Change Request and Release planning and execution for M&E Phase
- Deployment of product tools including the issue reporting system and secure FTP site, the action item tracking tool, and the collaboration web site
- Deployment of the Help Desk contact infrastructure
- Confirm all needed access and NCID credentials for State MIS support
- Submit requests for all needed access to cloud hosted environments for Crossroads system support
- Obtain and submit signed Non-Disclosure Agreements within fifteen (15) Calendar days of Contract Award for all Vendor staff who will have access to Crossroads Confidential Information

During the Maintenance and Enhancement phase, the primary services to be delivered for the Crossroads Product are the development, QA, UAT, and production deployment of major releases of the Crossroads system. These activities will take place during the Maintenance and Enhancement phase, which will begin on the first calendar day of the month after the Transition-In phase's closure. The plans and document deliverables will define the activities for this phase and the Schedule approved during the Transition-In phase will document the timelines for each release and release-related activities.

In addition to the above release activities, Voyatek will provide ongoing Level 2 and 3 Help Desk support to state staff, support for the current Crossroads Universal Interface for EBT, and support for unknown defects or issues in the Crossroads system and routine support activities. If the State has not completed the upgrade to the latest version of the WUMEI prior to the start of the new contract, Voyatek will work with the State and the EBT Provider to complete the upgrade as well as any related technology changes at no additional cost.

Voyatek will perform all application maintenance, which refers to routine support activities that include corrective, adaptive, and perfective aspect changes.

The list of Product deliverables is shown in Table 4. For more information on these services and deliverables, refer to NC Crossroads M&E RFP 30-25002-DCFV and the Voyatek North Carolina Technical Proposal.

Table 4: List of Product Deliverables

ID	Name	Timeline	RFP Response Label
1	Transition-In Plan	Provided with bid response proposal	Appendix A: Transition-In Plan
2	Product Management Plan	Provided with bid response proposal	Appendix B: Product Management Plan
3A	Product Work Plan and Schedule DRAFT	Provided with bid response proposal	Appendix C: Product Work Plan and Schedule
3B	Product Work Plan and Schedule FINAL	During Transition-In, 45 Calendar Days after contract execution date	

ID	Name	Timeline	RFP Response Label
4	Quality Assurance Management Plan	Provided with bid response proposal	Appendix D: Quality Assurance Management Plan
5	Communication and Coordination Plan	Provided with bid response proposal	Appendix P: Communications and Coordination Plan
6	Maintenance and Enhancement Status Reports	Monthly during the life of the contract, aligned with monthly invoice	
7	UAT Readiness Reports	Weekly status calls with the first report being no later than 14 Calendar Days Prior to each UAT Start	
8	UAT Completion Reports and System Documentation	As coordinated with NC for each Deployment	
9	Production Deployment Plan	During Transition-In: 90 Calendar Days prior to the first statewide deployment	
10	Disaster Recovery and Contingency Plan	Draft plan provided with bid response proposal	Appendix F: Disaster Recovery and Contingency Plan
11	Security and Vulnerability Plan	Draft plan provided with bid response proposal	Appendix G: Security and Vulnerability Plan
12	Risks and Issues Management Plan	Provided with bid response proposal	Appendix H: Risks and Issues Management Plan
13	Configuration Management / Release Management Plan	Provided with bid response proposal	Appendix J: Configuration Management and Release Management Plan
14	Evidence of Vendor and financial stability (See Section V for acceptable documentation)	Provided with bid response proposal	Appendix K: Evidence of Vendor Financial Stability
15	Transition-Out Plan	Provided with bid response proposal	Appendix L: Transition-Out Plan

ID	Name	Timeline	RFP Response Label
16	Transition-Out Completion Report	No later than 10 days prior to the contract end date	
17	Partnerships and Contractual Relationships	During Transition-In	Appendix M: Partnerships and Contractual Relationships
18	Risk and Security Assessment of Vendor critical systems and infrastructure	Assessment due during Transition-In Phase	
19	Help Desk Plan	Provided with bid response proposal	Appendix N: Help Desk Plan
20	Rehosting Implementation and Rollout Plan	Provided with bid response proposal	Appendix E: Rehosting Implementation and Rollout Plan
21	Vendor Hosting Status Report	Monthly during the life of the contract, aligned with monthly invoicing	

2.2 Exclusions

The following services are out of scope for this procurement:

- Production of Electronic Benefit Transfer (EBT) cards and the actual processing of EBT cards at authorized vendors/retailers.
- Any changes to modify or enhance the system not listed in the contract, not identified during the JAD sessions, or mutually agreed to by both parties.

2.3 Assumptions

- North Carolina DHHS staff assigned to this project will commit to the project goals and objectives.
- North Carolina DHSS staff will review and approve deliverables in a time-boxed manner. The review period for each document deliverable will be a minimum of five (5) business days for initial feedback, as determined by the Crossroads WIC MIS Release Manager. The revision period will be determined by Voyatek. The review period for final comments/approval will be four (4) business days unless otherwise directed by the Crossroads WIC MIS Release Manager.
- The Crossroads WIC MIS Release Manager will be responsible for distributing project deliverables to appropriate stakeholders for sign off. The Crossroads WIC MIS Release Manager will facilitate review and approval activities/meetings if needed.
- North Carolina DHHS dependencies, such as policies and procedures, must be done prior to the Transition-In of the Crossroads system.

- North Carolina DHHS will be responsible for the WIC clinic equipment, network and internet connectivity for the duration of the Transition-In and Maintenance and Enhancement phases.
- Voyatek will be responsible for the application rehosting transition to the cloud, including the creation of the Azure instance, system deployment to the cloud, and management of Azure environments to support Crossroads production, staging, UAT, sandbox, reporting and disaster recovery.
- Creation and management of the Crossroads development and testing environment within the Voyatek designated facilities.

2.4 Project Facilities Location

The Voyatek NC Crossroads team is located at the Voyatek office located at:

Voyatek

9300 W. 110th St., Suite #200

Overland Park, KS 66210

The Voyatek Product Manager, Business Analyst Lead, Technical Oversight, and JAD and Training Support staff will work remote from their respective offices when not onsite at either North Carolina DHHS locations or in the Overland Park, KS office.

3. Schedule Management Plan

The project schedule is the roadmap for how the project will be executed. Schedules are an important part of any project as they provide the project team, sponsor, and stakeholders with a picture of the project's status at any given time. The purpose of the Schedule Management Plan is to define the approach the Voyatek Project Team will use in updating and maintaining the project schedule. This plan also includes how the team will monitor the project schedule and manage changes after the baseline schedule has been approved. This includes identifying, analyzing, documenting, prioritizing, approving or rejecting, and publishing all schedule-related changes. Changes to the Schedule Management Plan will be made within this document and approved as appropriate.

The Voyatek Product Manager will create the Voyatek Project Schedule in MS Project based on the deliverables identified in Voyatek's response to the North Carolina RFP solicitation. Activity definition will identify the specific work packages to be performed for each deliverable. Activity sequencing will be used to determine the order of work packages and assign relationships between project activities. Activity duration estimating will be used to calculate the number of work periods required to complete work packages. Resource estimating will be used to assign resources to work packages to complete schedule development.

Voyatek delivered a preliminary schedule with our response. During the Transition-In phase of the project, this preliminary schedule will be reviewed by the Voyatek Product Manager and any resources assigned to project tasks. The Voyatek Project Team must agree to the proposed work package assignments, durations, and schedule. Once Voyatek has confirmed the work package assignments, durations and schedule, the Voyatek Product Manager will deliver the schedule to the Crossroads WIC MIS Release Manager for North Carolina WIC's review and approval.

Note, the Crossroads WIC MIS Release Manager may have a separate project schedule that contains the tasks for DHHS staff directly or indirectly related to Voyatek's schedule. The Crossroads WIC MIS Release Manager and Voyatek Product Manager will work together to synchronize schedules as necessary to coordinate activities. After such changes have been agreed to, the Voyatek Product Manager will then baseline the approved schedule.

3.1 Roles and Responsibilities for Schedule Development

The Voyatek Product Manager will be responsible for facilitating work package definition, sequencing, and estimating duration and resources with the project team. The Voyatek Product Manager will also facilitate the maintenance of the project schedule using Microsoft Project and validate the schedule with the` Voyatek Project Team, stakeholders, and North Carolina WIC. The Voyatek Product Manager will obtain schedule approval from North Carolina and baseline the schedule.

The Voyatek Project Team is responsible for participating in work package definition, sequencing, and duration and resource estimating. The Voyatek Project Team will also review and validate the proposed schedule and perform assigned activities upon the approval of the change.

North Carolina will participate in review of the proposed schedule and approve the final schedule before it is baselined. The North Carolina WIC stakeholders will participate in reviews of the proposed schedule and assist in its validation as appropriate.

3.2 Schedule Control and Reporting

The Voyatek Product Manager is responsible for regularly reviewing the schedule updates/reviews; determining impacts of schedule variances; submitting schedule change requests; and reporting schedule status to the Crossroads WIC MIS Release Manager. The Voyatek Product Manager will review and update the schedule on at least a bi-weekly basis with actual start, actual finish, and completion percentages by task owners.

The Voyatek Project Team is responsible for participating in regularly scheduled updates/reviews; communicating any changes to actual start/finish dates to the Voyatek Product Manager; and participating in schedule variance resolution activities as needed.

The Voyatek status report will include a section specifically for reporting schedule status, significant impacts to project timeline, and any schedule change requests. North Carolina WIC will maintain awareness of the project schedule status and review/discuss any schedule change requests reported by the Voyatek Product Manager.

Should the need arise to modify the project schedule due to scope change or a significant impact to the timeline, the Voyatek Product Manager will modify the Voyatek schedule with clear indication of the changes made and walkthrough the modifications with the Crossroads WIC MIS Release Manager. The Voyatek Product Manager will document the agreement and will re-baseline the schedule based on any resulting agreement.

3.3 Schedule Changes and Thresholds

If any member of the Voyatek team determines that a change to the Voyatek schedule is necessary, they will communicate the change to the Voyatek Product Manager. Voyatek will meet to review and evaluate the change. The Voyatek Product Manager and Voyatek team must determine the tasks that will be impacted, assess the variance because of the potential change, and identify any alternatives or variance resolution activities that may be employed to determine how they would affect the scope, schedule, and resources. If, after this evaluation is complete, the Voyatek Product Manager determines that any change will exceed the established boundary conditions, then a schedule change request will be submitted to the Crossroads WIC MIS Release Manager.

Submittal of a Schedule Change Request is required if:

- The change is estimated to reduce the duration of the overall baseline schedule by 10% or more or increase the duration of the overall baseline schedule by 10% or more.

Schedule change requests that meet the above conditions will need to follow the change control process described earlier.

Once change requests have been reviewed and approved, the Voyatek Product Manager is responsible for adjusting the schedule and communicating all changes and impacts to the Voyatek Project Team and North Carolina WIC. The Voyatek Product Manager will archive the change request in the project records repository.

4. Staffing Management Plan

This Staffing Management Plan describes how Voyatek will staff to meet the project, business, and technical obligations over the entire lifecycle of transitioning the support, maintenance, and enhancement of the North Carolina Crossroads system.

The Staffing Management Plan details the project’s human resources requirements and how those requirements will be fulfilled. The Staffing Management Plan includes the following sections:

- Project Roles and Responsibilities - summarizes the responsibilities for each role required to conduct the project work
- Responsibility and Assignments - includes the project’s RACI Matrix
- Acquisition Strategy - describes when, how, and from what sources staffing will be acquired
- Organization Chart - displays project reporting relationships

Changes to the Staffing Management Plan will be made within this document and approved as appropriate.

4.1 Roles and Responsibilities

The key to a successful project is the employment of experienced and well-trained staff. The Crossroads Product will benefit from superior staff—professionals with many years of relevant experience. Voyatek staff is unique in the world of WIC system development, given our practical, operational, and technical experience in the WIC arena. Our staff focus solely on managing and developing only WIC information system projects. We will support the Crossroads system with knowledge of how WIC professionals provide nutrition assessment and education and awareness of how the system impacts operations at the Clinic and State levels. Because of our wealth of “real world” knowledge, Voyatek builds and supports WIC information systems that work for WIC staff. The roles for this project are:

Product Manager

The Voyatek product manager is responsible for overall project execution and accomplishment of all project deliverables. The product manager will manage the daily work of the Voyatek team and coordinate contract work with North Carolina WIC.

Responsibilities include:

- Serve as the primary point of contact for the contract and project for North Carolina WIC and other NC entities
- Provide both contract administration and project management throughout the contract
- Coordinate Voyatek resources for execution of the WIC MIS project with full authority to commit Voyatek on matters concerning the contract
- Confirms that all project deliverables and services are provided on time, within scope and within budget
- Develop project plans and objectives, involving all relevant stakeholders and ensuring technical feasibility
- Ensure resource availability and allocation
- Develop a detailed project plan to track progress

- Use appropriate verification techniques to manage changes in project scope, schedule, and costs
- Measure project performance using appropriate systems, tools, and techniques
- Report and escalate to management as needed
- Manage the relationship with North Carolina WIC and all stakeholders
- Perform risk management to minimize project risks
- Establish and maintain relationships with third parties/vendors when needed
- Create and maintain comprehensive project management documentation
- Notify the DHHS Release Manager, verbally within one business hour and in writing within one business day, when Voyatek discovers any problem(s) that may jeopardize the successful or timely completion of our contract obligations.

Business Analyst Manager

The Voyatek Business Analyst Manager will lead business analysis activity throughout the contract.

Responsibilities include:

- Manage the overall requirements and requirements verification process
- Lead and create change request responses and estimates
- Provide daily technical guidance for the business analysts
- Work with well-established processes in a team environment
- Verify that workflow in the system is optimized
- Verify that customer requirements are accurately reflected in the system and in system documentation
- Validate that test scripts fully satisfy North Carolina's business requirements and needs
- Support the North Carolina Help Desk, including assisting with data corrections

Development Manager

The Voyatek Development Manager will provide leadership for the technical team throughout the contract, including the important Transition-In work to rehost the NC Crossroads system to the Azure cloud.

Responsibilities include:

- Manage the software build baseline, including management of system configuration and architecture changes
- Provide daily technical guidance for the development team
- Develop necessary user interface software to meet requirements, including maintaining and enhancing the critical interface to the EBT system.
- Develop necessary system interface software to meet requirements
- Develop necessary software/scripts to manage database layer
- Develop necessary software to manage business operations layer
- Verify the optimal utilization of technology and engineering resources to meet customer requirements.
- Maintain and support the system design for approved enhancements

Test Manager

The Voyatek Test Manager will provide leadership for the testing team throughout the contract, including managing all testing efforts, including end-to-end system testing, regression testing, and performance testing.

Responsibilities include:

- Manage the overall end-to-end system testing processes during maintenance and enhancement phases inclusive of User Acceptance Testing (UAT)
- Maintain and manage well-established test processes in a team environment
- Test highly complex code and integrated system capabilities
- Confirm that the system functions correctly across different environments
- Conduct tests to verify user functionality and system configuration
- Investigate and resolve matters of significance for end-user problems
- Write test scripts, test reports, requirement documents and other related technical documents
- Produce test reports to summarize all testing activities for clients

Technical Oversight

Responsible for the technical architecture and ensuring that a solution is implemented to meet all system and security requirements.

Responsibilities include:

- Providing technical direction and guidance, as well as hands-on project management, for all product and software development
- Ensuring the optimal application of technology and engineering resources to meet customer requirements
- Ensuring that the product is fully and correctly defined and documented
- Ensuring implementation of formal processes to support the product

Training Lead

Responsible for defining training needs, developing training curricula, and oversight of training delivery, as requested by NC.

Responsibilities include:

- Lead the training efforts associated with deploying a new system to system users at customer clinics
- Monitor, evaluate and record training activities and program effectiveness
- Assess training needs through surveys, interviews with employees, focus groups, or consultation with managers, instructors, or customer representatives
- Organize and develop, or obtain, training procedure manuals and guides and course materials such as handouts and visual materials

Software Developers

Provide the required software changes to accomplish the transfer of the system.

Responsibilities include:

- Develop necessary user interface software to meet requirements
- Develop necessary system interface software to meet requirements
- Develop necessary software/scripts to manage database layer
- Develop necessary software to manage business operations layer

Business Analysts

Provide the required work to refine business processes to validate all requirements are met.

Responsibilities include:

- Work with well-established processes in a team environment
- Validate that specifications capture customer needs
- Verify that workflow in the system is optimized
- Verify that customer requirements are accurately reflected in the system and in system documentation

Software Testers

Provide the required software testing to certify that all requirements are met.

Responsibilities include:

- Work with well-established processes in a team environment
- Test highly complex code and integrated capabilities
- Verify that web pages are functional across different environments
- Conduct tests to verify user functionality
- Investigate and resolve matters of significance for end-user problems and escalate if necessary
- Write test scripts, requirement documents and other related technical documents

Training Teams

Provide the required training to certify that all requirements are met.

Responsibilities include:

- Organize and develop, or obtain, training procedure manuals and guides and course materials such as handouts and visual materials
- Conduct classroom training for new users
- Assess training needs through surveys, interviews with employees, focus groups, or consultation with managers, instructors, or customer representatives

4.2 Responsibility and Assignments

The RACI Matrix is a tool to help identify roles and assign cross-functional responsibilities to a project deliverable or activity. RACI represents the level of involvement within the project: R - Responsible, A - Accountable, C - Consulted, and I – Informed.

RACI Definitions:

- Responsible - person or role responsible for ensuring that the item is completed
- Accountable - person or role responsible for actually doing or completing the work

- Consulted - person or role whose subject matter expertise is required to complete the item
- Informed - person or role that needs to be kept informed of the status of item completion

The table below is the initial RACI matrix for the North Carolina Crossroads Maintenance and Enhancement project. While this matrix provides an overall view of the roles necessary to complete the project, new roles or activities may be identified throughout the project, thus, the RACI matrix will be updated as needed. Voyatek Product Manager and the Crossroads WIC MIS Release Manager will mutually agree upon such updated versions as needed.

Table 5: RACI matrix for the North Carolina Crossroads Maintenance & Enhancement project

Deliverable/Task	Voyatek Role									
	Product Manager	Development Manager	Technical Oversight	Business Analyst Manager	Testing Manager	JAD & Training Support	Software Developers	Software Testers	Business Analysts	Training Teams
Kickoff Meeting	RA	A	A	A	A	I	I	I	I	I
Transition-In	RA	A	A	A	A	C	C	C	A	I
Product Management Plan	RA	C	C	C	C	C	C	I	I	I
Product Work Plan	RA	C	C	C	C	C	I	I	I	I
Schedule Management	RA	I	I	I	I	I	I	I	I	I
Quality Management	RA	A	A	A	A	A	A	A	A	A
Staffing Management	RA	C	C	C	C	C	I	I	I	I
Communications Management	RA	C	C	C	C	C	I	I	I	I
Risk and Issues Management	RA	C	C	C	C	C	C	C	C	C
System Design and Development Management	RA	A	A	A	C	I	C	C	C	I
Capacity Management	RA	A	A	C	C	I	AC	C	C	I
Status Reporting	RA	RA	A	RA	RA	A	A	A	A	A
Change Management	RA	A	A	A	A	C	C	I	I	I
Product Governance	RA	A	A	A	A	A	I	I	I	I

Deliverable/Task	Voyatek Role									
	Product Manager	Development Manager	Technical Oversight	Business Analyst Manager	Testing Manager	JAD & Training Support	Software Developers	Software Testers	Business Analysts	Training Teams
Training Management	RA	C	C	C	I	RA	I	I	I	A
Test Management	RA	C	C	C	RA	I	I	A	C	I
Security and Vulnerability Management	RA	RA	A	A	A	I	A	A	C	I
Disaster Recovery	RA	C	C	C	C	I	I	I	I	I
Help Desk Support	RA	A	A	A	A	I	I	I	I	I
Action Items	RA	A	A	A	A	A	A	A	A	A
Release Management	RA	A	A	A	A	C	C	C	C	I
Documents, Deliverables, and Records Management	RA	A	A	A	A	A	A	A	A	A
Collaboration Web Site	RA	RA	A	RA	RA	RA	A	A	A	A
NC Technical Architecture System Design (TASD)	RA	A	RA	C	C	I	C	C	C	I
Transition-Out	RA	A	A	A	A	A	I	I	I	I

4.3 Acquisition Strategy

Voyatek has staffed all key positions on the contract with the employees who were currently supporting NC WIC and the Crossroads system. These staff are highly experienced and uniquely qualified to support NC WIC and the Crossroads system. Voyatek's ongoing commitment is to provide staff who have the skill set to meet the needs of the Crossroads Maintenance and Enhancement project. No recruiting is necessary to maintain the primary team.

While we do not anticipate a change in staffing from the proposed personnel, Voyatek understands that unforeseen circumstances may require resource shifts. Since our original contract with North Carolina, Voyatek has become the sole maintenance and operations, and enhancement vendor for all states using the Crossroads system. This has increased our ability to provide a resource pool of qualified individuals available to support the project in the event key staff changes are required. In these circumstances, the Product Manager will identify a staff member with comparable skills and availability to perform tasks and present North Carolina WIC with a resume for approval prior to replacing the staff member.

Voyatek recognizes the contractual requirements, as appropriate, to present new staff resumes to North Carolina WIC for review and support interviewing of key staff. Voyatek acknowledges the State's option to reject proposed staff if that staff person is found to not have the necessary skills or is otherwise not acceptable to North Carolina.

4.4 Organization Chart

In assembling the team for the North Carolina Crossroads Maintenance and Enhancement project we have selected experienced project management, software developers and project staff familiar with WIC and experienced with the Crossroads system. The following chart presents the team assigned to supporting the Crossroads system. Additional personnel may be added as needed during more intense development and testing activities of the project.

All named positions identified in our organizational chart are staffed with existing employees who were selected based on their experience and familiarity with Crossroads and/or the latest implementation and operations of our other WIC projects. Please note that a letter of intent was submitted with our response for the Business Analyst Manager. All staff are immediately available for contract start.

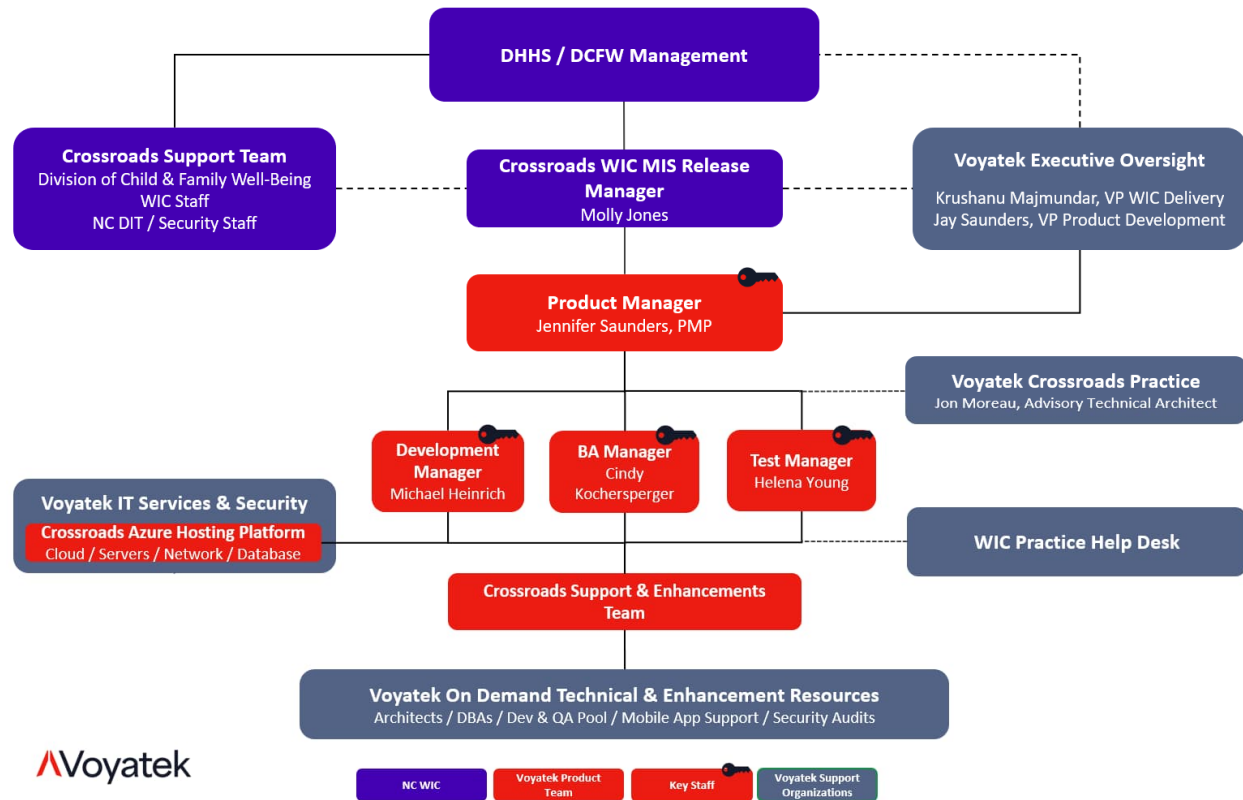


Figure 1: North Carolina Crossroads MIS Product Team Organization Chart

5. Product Work Plan and Schedule

Voyatek will deliver a draft of the Product Work Plan and Schedule with our response. The Product Work Plan describes our process, frequency, and format for providing and maintaining the Product Work Plan and will cover the following information:

- Detailed product schedule including tasks required for Transition-In, the modification and deployment of Crossroads Change Requests and System Releases, and Transition-Out.
- Work Breakdown Structure (WBS) providing a graphic depiction that defines the tasks associated with the objectives for the entire scope of the contract. The WBS will be a decomposition of the work to be executed by the entire product team and indicate task dependencies along with start and end dates. The WBS will include all product deliverables, milestones, and activities at a level that allows the State to track progress towards completion.
- Product tasks and deliverables describing what is required to accomplish the work detailed in the WBS

The Product Work Plan is a stand-alone document (refer to Appendix C – Product Work Plan and Schedule) and will be reviewed, approved, and maintained outside of this Product Management Plan. The draft schedule, also a stand-alone file, provided with Voyatek’s RFP response will serve as the starting point and will be maintained throughout the project by the Voyatek Product Manager utilizing a version of MS Project that meets North Carolina’s requirements at the time of Transition-In.

The Schedule Management plan within this section defines the approach the Voyatek Product Manager will use in creating the schedule. This plan includes how the Voyatek Product Manager will monitor the project schedule and manage changes after the baseline schedule has been approved. This includes identifying, analyzing, documenting, prioritizing, approving or rejecting, and publishing all schedule-related changes.

6. Quality Management

The Quality Assurance Management Plan (QAMP) for the North Carolina Crossroads Maintenance and Enhancement Product will establish the activities, processes, and procedures for ensuring a quality product upon the conclusion of the project. The QAMP defines the activities and processes related to managing the quality of the project. The plan is applicable to the software development lifecycle of the application for the Crossroads system. This includes project management, analysis, business process re-engineering, design, configuration, modification, extension, data conversion, testing, pilot, installation, implementation, training, and post-implementation and support of the application.

The purpose of the Quality Assurance Management Plan is to establish the goals, processes, and responsibilities required to implement effective quality management functions for the project. The QAMP defines how the Voyatek Project Team will implement, support, and communicate project quality practices. The QAMP will accomplish the following objectives:

- Outline the purpose & scope of quality activities
- Define how quality will be planned and managed
- Define quality assurance (QA) activities
- Define quality control (QC) activities
- Define acceptable quality standards
- Define roles and responsibilities for quality management activities

The Quality Assurance Management Plan is a stand-alone document provided with our response (refer to Appendix D – Quality Assurance Management Plan). The review, update and maintenance of this plan will be performed separately from this document.

7. Communications Management

The Voyatek Product Manager will take a proactive role in facilitating effective communications throughout this project. The Voyatek Product Manager will be responsible for keeping the Crossroads WIC MIS Release Manager apprised of the current project status. This includes task and deliverable progress, identified issues, recommended resolutions and action items.

During the project, several forms of communication will occur to address scope, schedule, budget, status, assignments, issues, risks, change control, etc. Formal and informal mechanisms will be used to convey project information on a daily, weekly, monthly, or periodic as-needed basis throughout the lifecycle of the project.

The Communication and Coordination Plan is key to facilitating a successful project. This plan not only sets the expectations for formal communications but also describes our approach to handling issues and defines the escalation process. The Plan will describe the communication approach, including events such as status reports, conference calls, on-site visits, etc. Additional content will include identification of all stakeholders involved in the project, including the State, State contracted IV&V staff, the WIC EBT Contractor, the local WIC agencies/clinics, the prime contractor and its subcontractors, and other major related parties. The Communication and Coordination Plan will detail how communications between stakeholders will be delivered and managed.

Voyatek has submitted the Communication and Coordination Plan with our proposal as a stand-alone document (refer to Appendix P – Communications and Coordination Plan). The review, update and maintenance of the Communication and Coordination Plan will be managed as a separate document.

8. Risk and Issues Management

As with any project such as this, there are several risks involved that can impact the cost and/or the schedule. Consequently, the management of these risks is a critical phase of any project. Risks can occur across multiple areas and responsibilities – North Carolina WIC, Voyatek, and FNS, for example. For purposes of this plan, risks will be limited to those that Voyatek has some degree of control over.

A risk is an event or condition that, if it occurs, could have a positive or negative effect on a project's objectives. The purpose of the Risk Management Plan for North Carolina Crossroads Maintenance and Enhancement project is to establish the framework in which the Voyatek Project Team will identify risks and develop strategies to mitigate or avoid those risks. This plan also defines how risks associated with the project will be recorded and monitored throughout the lifecycle of the project.

This Risk Management Plan includes the following sections:

- Risk Management Approach – Deciding how to approach and conduct the risk management activities for the project
- Roles & Responsibilities – Defining how each team role contributes to managing the risk process
- Risk Identification – An initial and continuous effort to identify, quantify and document risks as they are identified.
- Risk Prioritization & Categorization – Evaluate identified risks to determine probability of occurrence, impact, and timeframe.
- Risk Response Planning - Establish an action plan for risk and assign responsibility.
- Risk Monitoring, Controlling & Reporting – Capture, compile, and report risk using the Risk Register

The Risk and Issues Management Plan has been submitted with our response (refer to Appendix H – Risks and Issues Management Plan). The review, update and maintenance of the Risk and Issue Management Plan will be managed as a separate document.

9. Collaboration Web Site

Voyatek maintains a SharePoint site for all projects which will be used to provide updates, archive various reports, documents, deliverables and conduct project communications. This platform enables senior management and stakeholders to access project data and communications at any point. SharePoint also allows stakeholders and project team members to collaborate on project work and communication.

9.1 Documents, Deliverables, and Records Management

The Configuration and Release Management Plan will govern the management of documents and versioning. Voyatek team members are familiar with Crossroads documentation and will develop an organized model to store historical and actively maintained documentation within the North Carolina SharePoint site. The site will allow users to check out documents, perform edits, check in changes, and track document revisions. This will allow for improved abilities to maintain documentation and to track current versions as changes are made.

Each document will contain a section for Version History. This history will maintain a version number, author name, and date for each document update. Voyatek staff responsible for document updates will be trained to update this information as part of each update. Key project staff are familiar with Crossroads documentation and version management.

In addition to maintaining version history within documents, Voyatek utilizes Microsoft SharePoint to track all document changes. North Carolina will receive access to a dedicated private SharePoint folder where all project documents will be located. Voyatek will provide authorized North Carolina staff direct access to the SharePoint site. If the user already has a Microsoft 365 account, they will be able to use the same login/password to the Voyatek portal.

SharePoint offers a variety of helpful features. Users can download documents, upload documents, follow documents to be notified of changes, share documents, edit documents from within their web browser, and share links to documents instead of emailing them directly. Documentation will be organized in a folder structure to allow for organization of files to meet North Carolina's needs.

The SharePoint portal will also maintain a full editing history for all document changes. This feature allows users to view prior versions, identify when changes have been made, and to recover lost content in the case of error.

SharePoint is integrated with Microsoft's Team Foundation Studio products. As needed, SharePoint can be integrated to serve as a repository for release notes, release installation packages, and other project materials.

9.2 Action Item Tracking Tool

The Action Item List will be set up in SharePoint and shared with project team members and other users as approved by North Carolina.

The Action Item List will contain the Action Item ID, Task Name, Due Date, Assigned To, Comment and Created date. Additional columns may be added as appropriate. Action Items will be tracked until the item has been completed. Outstanding Action Items will be reported on in the Monthly Status Report if deemed to be a priority item.

10. Change Management

The Change Management Plan identifies the processes used to effectively manage and plan changes within the project. A change is defined as any activity that alters the scope, schedule, cost, or deliverables of the project. This plan establishes how to propose changes, how to accept changes, how to monitor changes and controlling changes to the Crossroads System. In addition, the procedures identified in this plan will govern changes to project software, project activities and project requirements, from project inception through completion of the contract.

Release management is tightly coupled with the change management process. Change management determines schedules and approves each individual change. Release management then combines these approved changes into logical packages (both process-related and technology-related changes), managing the frequency of changes to production and minimizing business disruption. Change management then authorizes the release. The NC Crossroads M&E project utilizes three types of releases as described below.

Development (Major) Release: changes that provide a major impact to the Crossroads System and require significant time to develop, test and implement. As requested in the RFP, Voyatek will deploy three major releases per year, one approximately every 120 calendar days. Change requests requiring over 300 calendar days would assume to be included in a major release, unless otherwise mutually agreed upon with NC WIC.

Maintenance Release: standard changes placed into scheduled service packs; for example, bi-monthly maintenance release. Change requests requiring less than 300 hours of effort would probably be included in these releases.

Emergency Release: changes immediately needed to be moved into production. These are done on short notice (production deployment as soon as within 5 calendar days) when a critical change is identified as part of the Incident Management process.

10.1 System Change Request Process

The System Change Request Process (CR) as described in the RPF will be followed for the duration of the project. Updates and changes to the process will be mutually agreed upon and approved by North Carolina as needed.

The table below provides a summary of the Change Request process, including roles and responsibilities.

Table 6: Change Request Process – Roles and Responsibilities

Process Step	State Role	Voyatek Role	Description/Disposition	Time Frame (cd=calendar days)
1. CR Initiation	State Initiate Request	Log & Track Request	High Level Description	N/A
2. CR Validation	Provide Clarifications	Validate CR	Ensure minimum information	N/A

Process Step	State Role	Voyatek Role	Description/ Disposition	Time Frame (cd=calendar days)
			required to proceed	
3. Initial Response	Provide Clarifications, Review and Approve/Hold/Withdraw Initial Response	Prepare Initial Response	Identify functions impacted and potential risks. High level design, and Estimated hours and Costs.	Within 15 cd
4. Authorize Detailed Analysis	Participate in JAD, Provide Clarifications, Review, Modify and Approve Draft CR, or Hold/Withdraw Request	Prepare Detailed Response & CR Draft Estimate	Detailed System Design document, and binding hour and cost estimates (CR Draft Estimate)	Changes less than 300 hr. within 15 cd, otherwise 30 cd
5. CR Authorization	Review, Approve or Hold CR	Track/ Execute CR	Execute change, and prepare for deployment	Within 30 cd, longer if FNS approval necessary
7. CR Deployment	Discuss CR deployment with Voyatek	Mutually agree on a Deployment Schedule	Schedule CR Release as requested	Less than 300 hr. within 60 cd, otherwise 90 cd

10.2 CR Initiation, CR Validation, and Initial Response

Change Request (CR) Concepts will be primarily initiated by North Carolina and submitted in writing to the Voyatek Product Manager. The CR Concept will be a high-level description of the desired change. NC WIC will log the CR in Azure DevOps.

Voyatek will review the CR Concept, confirm the minimum information required to proceed is available in the request and ask for clarifications when needed from the State.

Voyatek's review will Identify functions impacted by the proposed change and potential risks associated with the change. Voyatek will submit the initial response for State review and approval within fifteen (15) calendar days of receiving the CR Concept. The CR Response will include the Voyatek's understanding of the original CR Concept with high-level detail like content provided in the original CR Concept, and a high-level non-binding system design outlining what Crossroads functions and screens are affected, list of design assumptions if applicable, and the conceptual estimate of hours and cost.

10.3 Authorize Detailed Analysis and CR Authorization

North Carolina will review, modify and approve the initial CR Response then notify the Voyatek Product Manager of the approval, hold or withdrawal of the CR from the backlog. For approved initial CR response, Voyatek will then initiate detailed analysis of the change and prepare a detailed system design document. Detailed analysis may include asking the State additional clarifying questions, holding JAD discussions with NC WIC SMEs, or requesting feedback on an initial draft of the design. Based on detailed analysis activities, Voyatek will determine the binding hour and cost estimates (CR Draft Estimate) based on the modified and approved CR Response.

Voyatek will submit the CR Draft Estimate within:

- Fifteen (15) calendar days of receiving North Carolina's approval of the CR Response for CRs estimated at less than 300 hours of effort, as estimated by Voyatek
- Thirty (30) calendar days of receiving North Carolina's approval of a CR Response for which Voyatek estimates will require three hundred (300) hours or more to complete (Major CR).

North Carolina will review the CR Draft Estimate and notify Voyatek within thirty (30) calendar days, or longer if USDA/FNS approval of the CR Draft Estimate is required, whether the CR Draft Estimate is approved, requires further rework, put on hold, or withdrawn. Approved CR Draft Estimates will be signed by the State and returned to Voyatek. Voyatek will then sign and return the CR Draft Estimate to North Carolina.

Hour estimates for both approved and unapproved CR Draft Estimates put on hold will be binding for the duration of the Contract, including carryover into optional years.

The Voyatek Product Manager will update the CR log with the status of the CR, update the Schedule and the Product Work Plan as appropriate, and include the status of the CR in the monthly status report.

10.4 CR Deployment

North Carolina and Voyatek will mutually agree upon a deployment schedule for the approved CR Estimates considering the three types of releases identified below as well as the urgency of the change and the need to meet Federal deployment deadlines as appropriate.

Once all work is completed on the approved CR and the CR has been implemented, the Voyatek Product Manager will change the status of the CR in the change control log to "Implemented."

The Voyatek product team will update all project documents impacted by the change and identified in the CR. Once the updated documents are approved, they will be uploaded to the product library.

10.5 Changes to Reference Tables

Activities that can typically be completed independent of a production release (e.g., data set expansions, data purges) are completed on a more frequent basis (e.g., daily, or weekly) as agreed with the State. This also includes changes to reference tables which will be initiated by a CR from the State and a corresponding CR Response from Voyatek. This will not require detailed system design documents unless the CR affects existing System Documentation.

All reference table changes will be completed within five (5) Calendar Days of State approval of the CR Response, and at no additional cost to the State.

10.6 Changes Outside the Scope of the RFP

As per the RFP, changes to the System that are outside of the scope of this RFP, Voyatek's proposal, and the existing Crossroads Detailed Functional Design Documentation will be considered for additional cost and will go through the full change request process described above.

As per the RFP, Changes to the EBT interface, including FMNP, will be implemented by Voyatek at no additional cost to the State. Such changes will be initiated by a CR Concept from the State and a corresponding CR Response and CR Draft Estimate will be provided by Voyatek.

10.7 Corrections / Defect Fixes to Correct Deficiencies

As per the RFP, corrections / defect fixes to correct deficiencies based on the most recently updated published System design documentation (or implemented CRs/estimates where documentation has not yet been updated) are subject to the change request process but at no additional cost.

Voyatek's approach to defect fixes is described in detail in our response and summarized in the table below.

Table 7: Defect Priority Classification

Issue Priority Level	Classification	Priority Description	Issue Resolution Timeframe
1	Critical	Critical Component Failure: Does not allow testing to continue Major malfunction in the System	Within hours
2	Major	Major Component Failure: Does not allow testing to continue Defect or malfunction in certain areas of the System Problem must be resolved	Resolution within one business day
3	Medium	Medium Functional Problem: Testing can continue Functions in certain components do not work properly Components can still work with other components of the System	Resolution within 5 business days or as agreed
4	Minor	Minor Issue: Testing can continue Minor editing error found in a System component	Resolution in the next Planned Release
5	Trivial	Trivial Issue: Testing can continue Design Clarification issue Future enhancement to the System Cosmetic change needed	Not time sensitive, fix as time is available

10.8 Document Updates

Voyatek will provide the State timely updates to appropriate System documentation.

10.9 Document Update Process

Voyatek Quality Assurance Management Plan describes in detail our approach to quality assurance; designed to facilitate the timely updated of the appropriate documentation. Also, the Deployment Readiness Checklist will facilitate tracking that all relevant documentation is up-to-date.

10.10 Process to Log and Track pending CRs

Voyatek will use MS Azure DevOps and capabilities along with our SharePoint environment and capabilities to log and track the CRs. This will include the following information:

- An assigned sequence number
- A short description of the requested change
- Whether the change is a table change, code change, or other
- The date of the original CR from the State
- The date the CR Response was sent to the State
- The date the CR Response was approved/not approved by the State
- The date the CR Estimate was submitted to the State
- The date the CR Estimate was approved/not approved/put on hold by the State
- The binding hours and cost of the change
- The proposed delivery date for UAT of the completed Change Request
- Comments section
- Current version of any associated document

Voyatek will provide invoices for CRs that are at additional cost to the State. Voyatek acknowledges that the State may defer acceptance of CR solutions until the CR solution, and any required defect corrections, are implemented in the production environment.

11. System Design and Development Management

The Production Deployment Plan will provide a detailed description of the System Design and Development Management for the Crossroads application. This plan will be developed during the Transition-In phase and submitted to North Carolina 90 days prior to the first statewide deployment. This plan will include the procedures, detailed schedules, and resources needed to implement and immediately support each release of Crossroads statewide.

Additional topics included in this plan will be the software build tools, the process for requirements gathering, design validation and the development for each of the three types of releases:

Development (Major) Release: changes that provide a major impact to the Crossroads System and require significant time to develop, test and implement. As requested in the RFP, Voyatek is planning to deploy three major releases per year, one every approximately 120 calendar days. Change requests requiring over 300 hours would probably fit best in one of these releases, unless otherwise advised by the NC WIC.

Maintenance Release: standard changes placed into scheduled service packs; for example, bi-monthly maintenance release. Change requests requiring less than 300 hours of effort would probably be included in one of these releases.

Emergency Release: changes immediately needed to be moved into production. These are done on short notice (5 calendar days) when a critical change is identified as part of the Incident Management process.

11.1 NC Technical Architecture System Design (TASD)

As with all Crossroads documentation and artifacts, Voyatek assumes responsibility for the NC Technical Architecture System Design (TASD) created and maintained through the original Crossroads project. This document will be transitioned to the North Carolina SharePoint site. As part of the release cycle, Voyatek will review and update the TASD throughout the project, managing version control so that changes may be tracked.

11.2 Capacity Management

Based on Voyatek's understanding of the current hosting infrastructure, North Carolina should be able to accommodate up to 3% growth with relatively minor infrastructure changes. The primary potential for increased needs would be hardware to support data storage and SQL Server capacity as data volumes increase over time. For most other elements of the hosting infrastructure improved performance in new hardware as legacy hardware is replaced will exceed the growth rate in WIC participation.

Voyatek may be able to present options to North Carolina to increase hosting capacity while reducing the number of virtual servers, reducing licensing costs, and decreasing costs associated with environment maintenance. Voyatek will generate technical specifications for needed hardware and software as required for DHHS Information Technology Staff. Assistance can also be provided to map project requirements to standardized hardware options utilized in State data centers.

Voyatek maintains environment hosting capacity to support 11 major WIC programs. This infrastructure is intended to allow teams to generate development and testing environments as needed. The available remaining capacity is monitored, and additional infrastructure is added before

capacity limitations impact project needs. The hosting infrastructure will be evaluated at contract award, and with any other contract awards, so that it can be increased as needed. Voyatek has no limitations on procurement options and should a need arise, the purchase and expedited shipping of necessary hardware can be performed immediately.

11.3 System Documentation

Voyatek will assume responsibility for maintaining the Crossroads System Design documentation created and maintained through the original Crossroads project.

- Detailed Functional Design Documents (DFDD), including a detailed Risk Code Summary Matrix and Trigger Summary
- User Manuals
- Detailed Technical Specifications (DTS), including Data Dictionary (currently available in PDF format) and a detailed listing of all System Tables
- Crossroads Interface Control Document (ICD) for the NC Crossroads MIS-EBT Interface
- External Communication Documentation (ECD)
- Report Definition Documentation (RDD)
- Installation and Configuration Instructions, including hardware and software prerequisites;
- Central Processing Site Operations Manual
- White Papers to provide written guidance to assist North Carolina with understanding or solving an issue

As noted in Section 9 Collaboration Web Site of this document, Crossroads documentation repository is hosted in the North Carolina project on Voyatek's SharePoint site.

These documents will be maintained in MS Office 2016 format with version control and made available for North Carolina to edit. Additionally, files used for creating embedded figures, diagrams, tables, or other non-editable components within the document will be stored in SharePoint with the relevant document and with version control.

Voyatek will regularly review and update this documentation throughout the project and provide to North Carolina in a timely manner prior to deployment of each major system release to reflect all software change requests and defect corrections.

12. Test Management

Voyatek will create and maintain a comprehensive Test Plan that addresses Subsystem Integration, System Qualification, Regression, Readiness Certification, User Acceptance, Formal Acceptance, and Pilot testing. The Test Plan structure, format, and content are subject to the State review and approval. The Voyatek has assigned a dedicated Testing Manager who will be responsible for the implementation of the Test Plan. The scope of the Test Plan will include:

- Integration of current Crossroads processes and standards
- Software testing strategy, methodology processes, standards and guidelines for all software testing, including conversion testing activities
- Specification of entrance and exit criteria for each of the test events
- Templates and standards for all testing artifacts and deliverables
- Definition of testing metrics and how the metrics are recorded and reported
- Description of the approach for regression testing based on an analysis of which parts of the System may be affected by proposed and designed changes to the System and other supporting technologies
- Standards for establishing traceability from requirements to test cases

The Voyatek Testing team will work with state to define and review test scenarios and test scripts that exercise each business process, system transaction, use case, and requirement as applicable to the test phase. The Test team will conduct a checklist-based peer review for each test case and script. We will document the process and activities to populate and manage data within each test environment. Voyatek generates test data/files as necessary during Integration Test and uses the system to generate test data and transactions in System Test and later test phases.

The Test Plan will be developed per the Project Schedule. The plan will be reviewed, approved and maintained outside of the Product Management Plan.

13. Configuration and Release Management

The Configuration Management and Release Management Plan describes processes for managing Crossroads system configuration, version control for release source code, release management processes, and coordination with the EBT vendor for the North Carolina Crossroads Maintenance and Enhancement project.

Voyatek will review this plan with North Carolina staff to determine best practices during the Transition In Phase. The Configuration and Release Management Plan describes our normal standard of practice for clients that we serve. Voyatek maintains configuration data for a variety of business and technical configuration components. These include:

- System settings
- Cross-reference tables
- Web.config files
- IIS/Server settings
- Other configuration data
- Document version control
- Source code version control
- Installation tools
- Test scripts

The Configuration Management and Release Management Plan is a stand-alone document. Voyatek has updated this plan to reflect the implementation of automated processes using Azure DevOps and Octopus deployment. This plan is provided with our response (refer to Appendix J – Configuration Management and Release Management Plan). The review, update and maintenance of this plan is managed separately from this document.

14. Security and Vulnerability Management

Voyatek is committed to maintaining the integrity and confidentiality of our States' WIC program data. To meet these needs, Voyatek performs an annual Service and Organizational Controls (SOC) 2 audit for our Laurel Maryland development center. The SOC 2 audit covers Trust Service Criteria for Security, Processing Integrity, and Confidentiality. This audit and the underlying policies, procedures, and controls cover all elements of the security controls requested within this plan.

The goal of Security and Vulnerability Plan is to reference the audited controls associated with each requested security and vulnerability management domain. Providing appropriate coverage to these topics goes beyond what can be provided within a plan document and must be maintained on an ongoing basis. This document will provide mapping of requested controls to existing corporate policies and artifacts.

In this plan, Voyatek will provide mapping between requested information and documentation which provides coverage for the requested areas of concern. Voyatek also maintains a library of supporting policies and procedures related to audit controls and security objectives. These policies are referenced within this document and will be available to North Carolina as needed following contract execution. The Security and Vulnerability Plan describes Voyatek's audited security and vulnerability management processes based on SOC 2 Trust Services principles. The North Carolina Crossroads Maintenance and Enhancement project will fall under the Voyatek security umbrella and be included in yearly SOC 2 audits following contract execution.

Voyatek has submitted a Sample Security and Vulnerability plan created and approved by the NC Connects project for CACFP (refer to Appendix G – Security and Vulnerability Plan). This sample will be used as template for the Crossroads Security and Vulnerability plan and will be updated with the specific Crossroads details when Voytek takes over hosting of the system. Additionally, we have included a copy of our 2024 Type 2 SOC 2 audit report, which was delivered with no adverse findings (refer to Appendix Q – GCOM-3Sigma WIC & Nutrition-2024-Type 2 SOC 2-Final Report). The 2025 reporting period ended on February 28, 2025 and the audit cycle is actively in progress as of the submission of our proposal. We anticipate that the 2025 Type 2 SOC 2 report will be available at the time of contract start.

15. Training Management

The Voyatek corporate philosophy places great emphasis on training. Throughout the North Carolina Crossroads M & E project, we will incorporate our training philosophy into our training programs:

”Tell me and I will forget; show me and I may remember; involve me and I will understand.”

The Voyatek training team has extensive experience in designing and delivering training that supports end users. Voyatek combines general training knowledge with specific programmatic knowledge to develop successful training. Voyatek’s approach draws upon the depth of our experience with WIC.

Through a proven, structured training approach, Voyatek will provide a learning path that facilitates the understanding for North Carolina staff in the operation and use of the new WIC system. Our approach includes building real-world examples that will be seen in clinics. This approach will be tailored to meet the State’s needs by working closely with the State’s WIC senior staff to confirm that course instruction for system trainers, end users, and technical support personnel is comprehensive, easily understood and meets as many real-world situations as possible. The development of each of the training activities entails the following steps:

- Curriculum Design
- Training Development
- Training Implementation

Upon request by the State, Voyatek will provide on-site training to the State UAT test team. The training will consist of a comprehensive overview of the functional processes of the system, with emphasis on new functionalities. While training may include a review of the UAT process as needed, Voyatek recommends the users participating in UAT training have familiarity with the system and have been a part of the project team throughout previous phases on the project.

Training scenarios will be provided for each function to be performed. Each scenario will be built upon one another as more system functions are thoroughly explained. Voyatek will work the State to ensure that the appropriate scenarios are included in each type of training.

During UAT, Voyatek on-site staff will support the State UAT Test Team with any technical assistance. For assistance with how to perform a functionality associated with a test script, team members will be directed to use the provided user training materials, and on-line help. Having the test team rely on the user training materials while conducting UAT, will identify any deficiencies in the training material; any such deficiencies will be corrected immediately prior to final acceptance of the training materials by the State.

16. Disaster Recovery and Contingency Plan

The Disaster Recovery and Contingency Plan describes processes for responding to a disaster impacting either Voyatek or North Carolina facilities used in the North Carolina Crossroads Maintenance and Enhancement project.

This plan outlines the disaster and recovery procedures for the North Carolina Maintenance and Enhancement project in the event of a disaster than impacts Voyatek facilities or operations. This plan is also intended to cover Voyatek support during a disaster recovery event impacting North Carolina facilities or operations. This plan covers the procedures for declaring a disaster and communicating with North Carolina staff, interim business operations, and steps to resume full operational capacity.

This plan will focus on the restoration of North Carolina contract services including:

- Crossroads development
- Access to source control
- Build and release management
- Crossroads testing
- Access to documentation
- Access to test environments
- Help desk support
- Telecommunications
- Project management and coordination

Voyatek has submitted a Sample Disaster Recovery plan created and approved for the NC Connects project with our response that will be used as template for the Crossroads Disaster Recovery Plan (refer to Appendix F – Disaster Recovery and Contingency Plan). The sample plan is specific to cloud hosting and will be updated with the specific Crossroads details when Voytek takes over hosting of the system. The Disaster Recovery Plan is a stand-alone document provided with our response. The review, update and maintenance of this plan will be performed separate from this document.

17. Partnerships and Contractual Relationships Plan

The Partnerships and Contractual Relationships Plan describes Voyatek’s approach to and processes for managing contractual partnerships. While we do not intend to employ subcontractors for this contract and our proposal does not include partnerships or contractual relationships, this plan will be implemented if during the contract it is necessary to engage in such to support the North Carolina Crossroads Maintenance and Enhancement project.

This plan will be created during the Transition-In Phase and will outline Voyatek’s partnerships and contractual relationships when engaging subcontractors to supplement our team for a project.

Voyatek has submitted the Partnerships and Contractual Relationships Plan in Appendix M – Partnerships and Contractual Relationships Plan. The Partnerships and Contractual Relationships Plan will be a stand-alone document and the review, update and maintenance of this plan will be performed separate from this document.

18. Help Desk Support

Voyatek will provide help desk support to central office staff in the maintenance of day-to-day operations of North Carolina Crossroads system and all of its components including, portal, interfaces, batches, data, applications, reports and correspondences through an Incident and Problem Management process. Incident and Problem Management are the two primary activities of an application support organization. When executed in a holistic and industrialized manner, they serve to maximize application availability while minimizing the cost of application support.

Voyatek's approach to supporting NC WIC is to provide a full-time, dedicated team with the skills and knowledge to answer questions, research issues, build queries, resolve batch errors and other activities that occur day-to-day. NC will have direct access to this team by phone, MS Teams messaging, and email. Voyatek NC Crossroads team members will regularly attend the Weekly Status and Weekly Topic Calls. It is our intent that NC will not have to use our WIC Help Desk. However, in the event that the state is not able to reach a Voyatek team member, Voyatek will provide the phone number for the Voyatek WIC Help Desk.

The Help Desk Plan describes the approach to providing help desk services for the North Carolina Crossroads Maintenance and Enhancement project. It covers the following topics:

- Voyatek's Support Model
- Help Desk Solution Capabilities
- Roles and Responsibilities for
 - o Help Desk Staff
 - o Technical Support
 - o Business Analyst Specialists
- Help Desk Processes and Procedures
 - o General Help Desk Procedures
 - o Specific Help Desk Procedures

Voyatek has submitted the Help Plan with our response (refer to Appendix N – Help Desk Plan), which will be managed as a separate document.

19. Transition-In Management

The Transition In Plan describes the activities during the Transition In Phase during which Voyatek will assume hosting responsibility for the North Carolina Crossroads system and continue providing Maintenance and Enhancement.

Voyatek plans to provide a smooth transition to a be the new Crossroads System Hosting provider. This plan outlines the steps needed to migrate Crossroads hosting into Voyatek’s established cloud infrastructure for providing Maintenance and Enhancement services.

The Transition-In Plan covers the following topics:

- Transition Communications
 - o Kickoff Meeting
- Phase Documentation Deliverables
- Product Work Plan and Schedule
- Maintenance and Enhancement Status Reports
- Staffing and Training
- Transfer of Materials
- Infrastructure Preparation

The Transition-In Plan has been submitted with our proposal (refer to Appendix A – Transition-In Plan). Voyatek anticipates that it will be reviewed, updated and maintained separate from this plan.

20. Transition-Out Management

The Transition Out Plan describes the activities during the Transition Out Phase during which Voyatek will assist the State and incoming contractor for the North Carolina Crossroads Hosting, Maintenance and Enhancement follow-on project.

The Transition-Out Plan outlines the steps needed to migrate Crossroads hosting, source code and project artifacts into a new provider's infrastructure for providing Hosting, Maintenance and Enhancement services. The following topics are covered in the plan:

- Transition Communications
 - o Kickoff Meeting
 - o Technical Coordination Sessions
 - o Change Request and Release Planning
- Transition Out Phase Documentation Deliverables
 - o Transition Out Completion Report
- Transition Out Phase Activities

The Transition-Out Plan is a stand-alone document provided with our response (refer to Appendix L – Transition Out Plan). Voyatek anticipates that it will be reviewed, updated and maintained separate from this plan.

Appendix C: Product Work Plan and Schedule

The following pages provide NC WIC the Product Work Plan and Schedule which describes the work activities and schedule for the North Carolina Crossroads Maintenance and Enhancement project.

State of North Carolina
Department of Health and Human Services
Division of Child and Family Well-Being



Crossroads MIS
Maintenance and Enhancement Services

North Carolina WIC Program

Appendix C
Product Work Plan and Schedule

Trademarks

Trademarked names may appear throughout this document. Rather than list the names and entities that own the trademarks or insert a trademark symbol with each mention of the trademarked name, the names are used only for editorial purposes and to the benefit of the trademark owner with no intention of infringing upon that trademark.

Contact Information

To request copies, suggest changes, or submit corrections, contact:

North Carolina Department of Health and Human Services**Division of Child and Family Well-being, WIC Program**

Attention: Molly Jones

Crossroads WIC Release Manager

Phone: 252-903-3951

Email: Molly.Jones@dhhs.nc.gov

Revision History

Date	Version	Revised By	Description
12/18/2018	0.1	Jay Saunders, Three Sigma Software	Draft version
3/6/2025	1.0	Jennifer Saunders, Voyatek	Submission for RFP 30-25002-DCFW

Deliverable Description

This Product Work Plan and Schedule describes the work activities and schedule for the North Carolina Crossroads Maintenance and Enhancement project.

Contents

1	Project Schedule Planning	3
1.1	Work Breakdown Structure Development.....	3
1.2	Activity Definition.....	3
1.3	Activity Sequencing	3
1.4	Activity Resource Estimating.....	4
1.5	Activity Duration Estimation	4
1.6	Schedule Development.....	4
1.7	Schedule Control	4
2	Schedule Management	5
3	Wave Planning	6
4	Work Breakdown Structure (WBS).....	8
5	Draft Schedule	10

Figures

Figure 1: Schedule Management Planning Framework	3
Figure 2: Rolling-Wave Planning Iterations	7
Figure 3: NC Crossroads M&E Schedule.....	9
Figure 4: Draft Project Schedule.....	11

1 Project Schedule Planning

Voyatek’s approach to the schedule planning and development is based on the PMBOK project planning framework shown below.

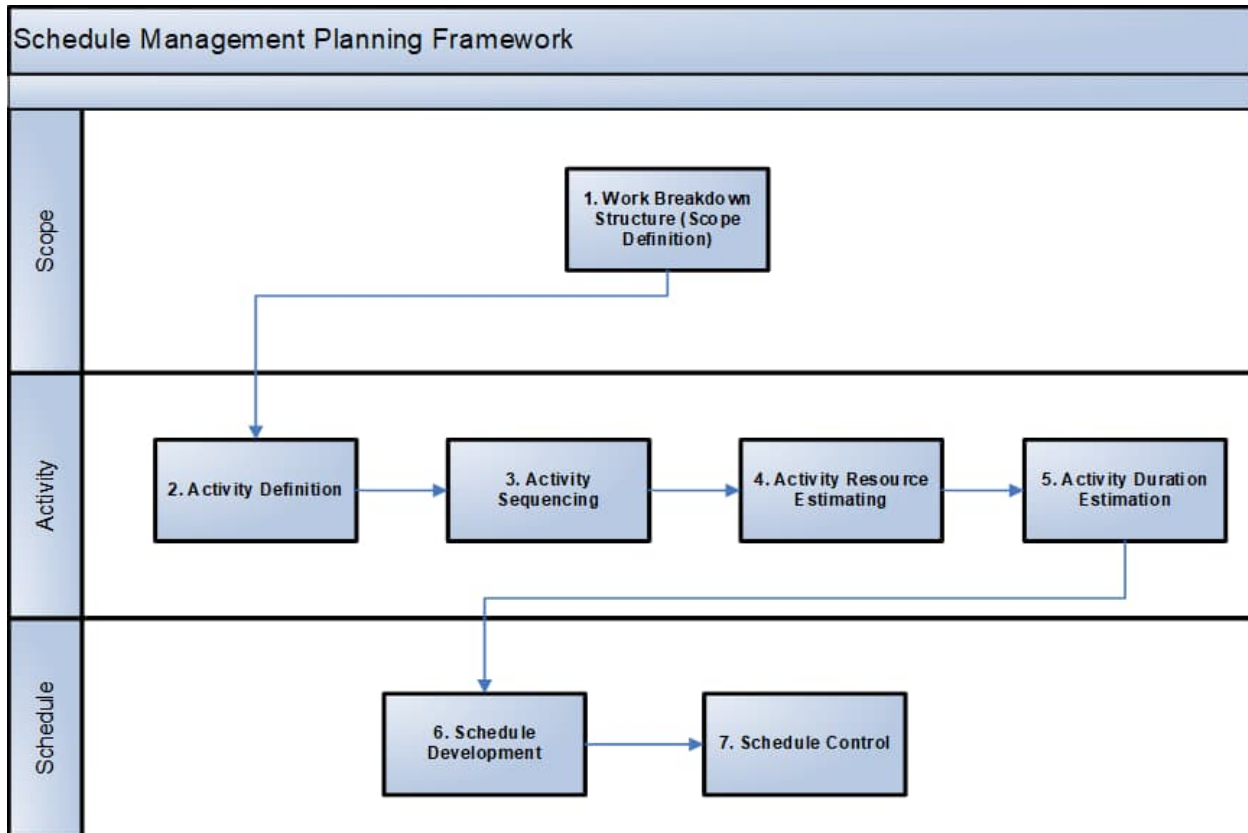


Figure 1: Schedule Management Planning Framework

1.1 Work Breakdown Structure Development

The schedule development begins with the definition of the products and services, or “deliverables” that make up the project. This is accomplished through a Work Breakdown Structure (WBS), represents the deliverables needed to complete the project. The WBS allows for the accumulation and summarization of schedule data necessary to track project progress.

1.2 Activity Definition

The Activity Definition process will identify the deliverables at the lowest level of the WBS, which is called the work package. A work package is made up of activities (or tasks) that must be accomplished to produce the deliverable.

Activities are represented as discrete units of work that require no more 120 hours to complete.

1.3 Activity Sequencing

The order in which activities need to occur is determined. Schedule activities can be logically sequenced using predecessors as well as leads and lags to support a realistic schedule with the

activity dependencies incorporated into the schedule. Resource Planning, Activity Definition, Activity Duration Estimation, and Activity Sequencing are typically closely-related planning activities, and may be performed in a single planning session.

1.4 Activity Resource Estimating

After deliverables are identified and organized in the WBS, the products and services are allocated to resources that will be responsible for performing the work.

1.5 Activity Duration Estimation

Based on the activity definition, an estimate is made of the amount of time required (duration) to complete the activity. A duration for the activity will be determined using the estimated effort, number of resources assigned to perform the work and the available work periods.

1.6 Schedule Development

As activities, predecessors, resource requirements, and durations are defined, the Schedule is produced. The output of this process is the Project Schedule.

1.7 Schedule Control

Once a schedule is baselined, any changes to dates and milestones will be subject to the Change Management process.

2 Schedule Management

The Draft Work Plan attached below was developed using MS Project 365. During the Transition-In Phase, the draft schedule will be reviewed, and finalized in consultation with the NC WIC, the Project Team, and interested stakeholders. The Voyatek Product Manager will work with the team to review tasks, time-line, deliverables and resources; in order obtain agreement from the team on assigned tasks and resources. Based on the team feedback the draft schedule will be updated based on priorities, critical path, resources, and estimated dates prior to baseline. Once the final draft has been approved by the State, the schedule is baselined and any changes to dates or milestones will require prior approval by the State.

The schedule will be updated bi-weekly as part of the status reporting process; and analyzed on monthly basis as part of the quality assurance process.

3 Wave Planning

It is not always feasible to create accurate projections and estimates through the end of multi-year projects. Beyond a certain time-frame, work plans and schedules become unrealistic due to the ever-increasing uncertainty of the future. To avoid investing resources and time in creating plans with unrealistic detail, the concept of “rolling-wave” planning is employed in developing the schedule. In rolling-wave planning, a top-down approach is used to assign WBS responsibility, budget, and duration to key organizational entities initially, but the detail is not created until the work is within a 6-month time frame.

The rolling-wave approach will be used for the NC WIC Crossroad Project. Rolling-wave planning iterations are scheduled quarterly. For each iteration, detailed bottom-up planning is done for cohesive, logical blocks of work to a six-month planning horizon, while work beyond this horizon will be planned at a higher level.

The Voyatek Product Manager will facilitate rolling-wave planning by scheduling the planning sessions and working with the State, project team, and other stakeholders, in order to define changes to current or new tasks, activities, and resources. The rolling-wave approach will coordinate, document, and communicate project resource and activity dependencies. The figure below depicts how the rolling-wave approach moves the detailed planning horizon into the future.

Rolling-wave planning will be based on a detailed planning horizon of the next six months. Activities scheduled to begin in the up-coming six months are planned in complete detail (near-term planning), while activities scheduled to start beyond the horizon are planned with less precision (long-range, high-level planning). Each rolling-wave begins with the planning of the tasks in near-term and long-range activities. The results of this optimization are captured, and the baselines are updated.

When the next planning date is reached, planning for the next iteration begins. Actual progress, change to project scope and/or budget, and status of project risks are all factored into that round of detailed and long-range planning. The expected outputs of a rolling-wave planning session include:

- Updated Project Schedule, to include all near-term activities
- Responsible Team Lead for each activity
- Resources (named individuals replacing the roles identified in high-level plans) allocated to the activities
- Milestones that will be used to report progress over the near term
- Updated task priorities
- Documentation of dependencies
- Documentation of external project dependencies
- Schedule baseline updated to include new activities (after initial baseline)

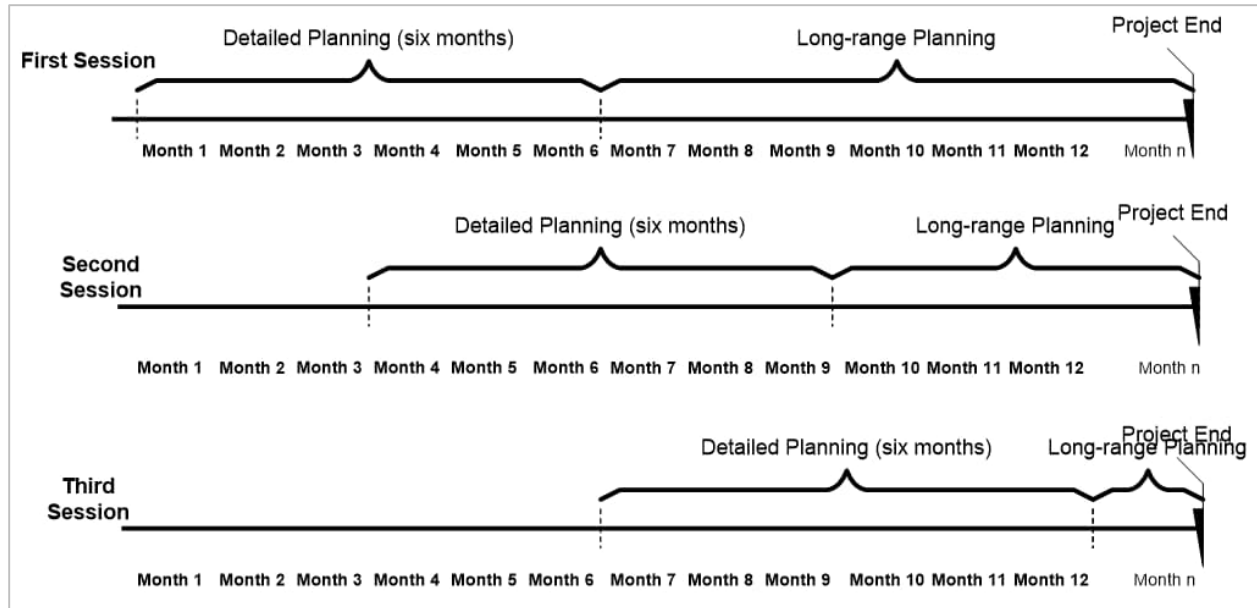


Figure 2: Rolling-Wave Planning Iterations

4 Work Breakdown Structure (WBS)

As requested in the RFP, a Work Breakdown Structure (WBS) that provides a graphical depiction that defines the tasks associated with the objectives for the entire scope of the contract is shown below. The WBS provides a decomposition of the work to be executed by the entire product team and indicate task dependencies along with start and end dates. The WBS includes product deliverables, milestones, and activities at a level which will allow the State to track progress towards completion. There are several ways to view a WBS graphically to reflect the hierarchical structure of the imbedded tasks. For the ongoing repetitive nature of system maintenance and enhancement (M&E) work, a Gantt view is a good way to look at the WBS because the work is cyclical. In the figure on the following page, the key elements of the services Voyatek will provide depicted in the Gantt view are:

- The contract starts August 1, 2025, as reflected in the RFP, with the Kickoff Meeting. The base period for the contract is seven years followed by up to three optional years, ending at maximum duration on July 31, 2035.
- The Transition-In Phase begins following the Kickoff Meeting and focuses on the rehosting of the system from the NC Data Center to the Azure Cloud. This is a 4-month effort.
- Also beginning after the Kickoff Meeting is the ongoing M&E for the Crossroads system. Due to the nature of the release planning for the first release to the cloud, some of this work must run in parallel with the Transition-In activities.
- Throughout the M&E Phase there are recurring activities that drive the release planning and delivery, including enhancements, as well as ongoing project management. The recurring tasks are:
 - o Weekly Status Meetings
 - o Monthly Status Reports
 - o Quarterly Schedule & Quality Reviews
 - o Monthly support activities for Crossroads Operations, Maintenance, & Hosting
 - o Regular system releases planned three times per year with a regular cadence for release design, development, UAT, and deployment
- At the end of the 7th year of the contract and at the end of each ensuing optional year is a possible Transition-Out period during which the Voyatek team may be turning over the responsibility for operating and hosting Crossroads to another entity.

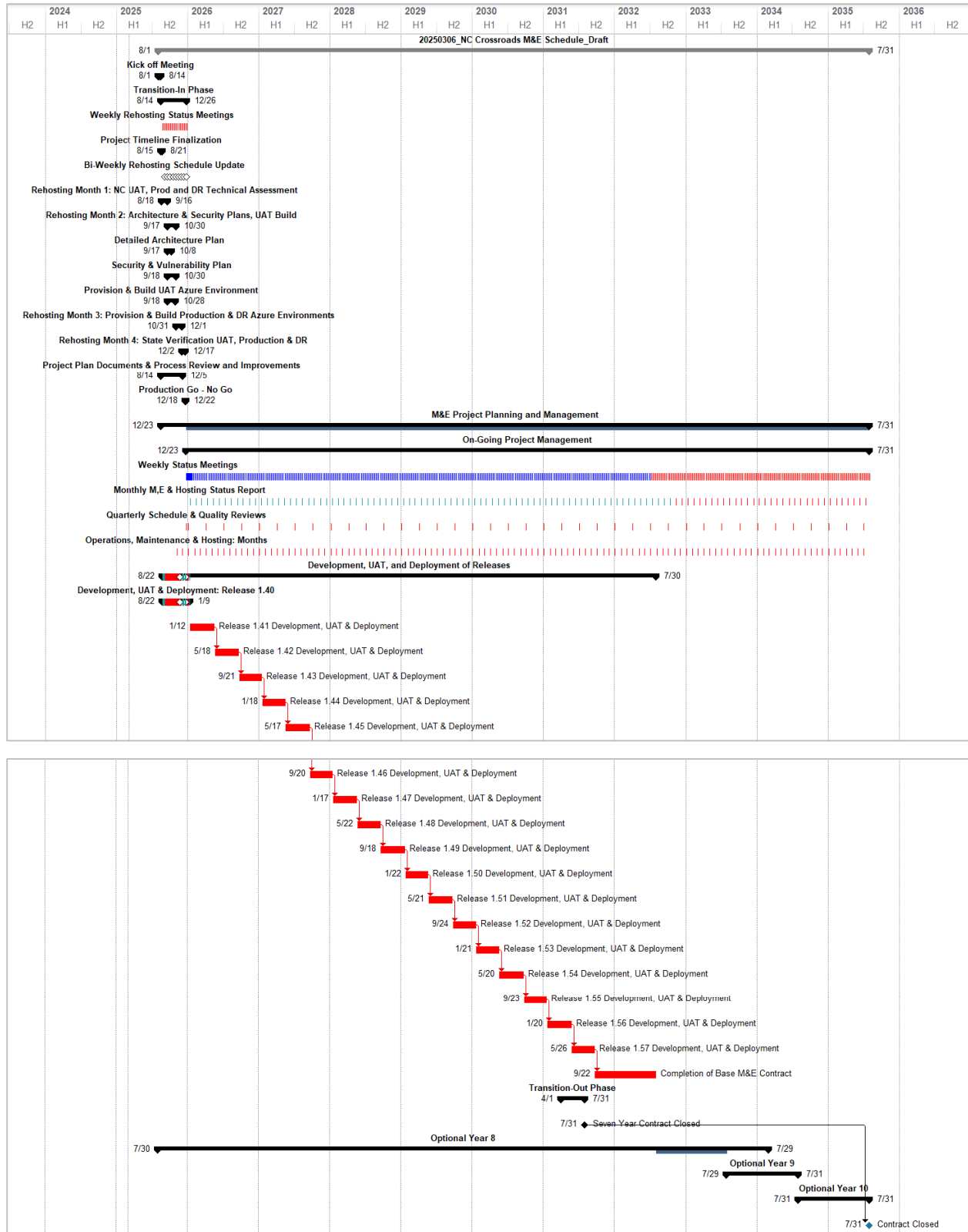


Figure 3: NC Crossroads M&E Schedule

5 Draft Schedule

The associated draft project schedule is presented on the following pages at a high level. Over the life of the project, the Voyatek Product Manager will provide the near-term portions of the schedule in greater detail to review with NC WIC as part of ongoing wave planning.

	Task Name	Duration	Start	Finish
0	20250306_NC Crossroads M&E Schedule_Draft	2608 days	Fri 8/1/25	Tue 7/31/35
1	1 Kick off Meeting	10 days	Fri 8/1/25	Thu 8/14/25
9	2 Transition-In Phase	95 days	Thu 8/14/25	Fri 12/26/25
10	2.1 Weekly Rehosting Status Meetings	90.07 days	Thu 8/21/25	Thu 12/25/25
30	2.2 Project Timeline Finalization	5 days	Fri 8/15/25	Thu 8/21/25
32	2.3 Bi-Weekly Rehosting Schedule Update	75 days	Wed 9/3/25	Fri 12/26/25
42	2.4 Rehosting Month 1: NC UAT, Prod and DR Technical Assessment	22 days	Mon 8/18/25	Tue 9/16/25
45	2.5 Rehosting Month 2: Architecture & Security Plans, UAT Build	32 days	Wed 9/17/25	Thu 10/30/25
46	2.5.1 Detailed Architecture Plan	16 days	Wed 9/17/25	Wed 10/8/25
53	2.5.2 Security & Vulnerability Plan	31 days	Thu 9/18/25	Thu 10/30/25
60	2.5.3 Provision & Build UAT Azure Environment	29 days	Thu 9/18/25	Tue 10/28/25
68	2.6 Rehosting Month 3: Provision & Build Production & DR Azure Environments	22 days	Fri 10/31/25	Mon 12/1/25
75	2.7 Rehosting Month 4: State Verification UAT, Production & DR	12 days	Tue 12/2/25	Wed 12/17/25
82	2.8 Project Plan Documents & Process Review and Improvements	81 days	Thu 8/14/25	Fri 12/5/25
87	2.9 Production Go - No Go	3 days	Thu 12/18/25	Mon 12/22/25
136	3 M&E Project Planning and Management	2508 days	Fri 8/15/25	Tue 7/31/35
137	3.1 On-Going Project Management	2421 days	Tue 12/23/25	Tue 7/31/35
138	3.1.1 Weekly Status Meetings	2506 days	Tue 12/23/25	Tue 7/31/35
659	3.1.2 Monthly M,E & Hosting Status Report	2396 days	Sat 1/10/26	Tue 7/10/35
775	3.1.3 Quarterly Schedule & Quality Reviews	2485 days	Tue 12/23/25	Mon 7/2/35
816	4 Operations, Maintenance & Hosting: Months	2521 days	Mon 11/3/25	Mon 7/2/35
934	5 Development, UAT, and Deployment of Releases	1726 days	Fri 8/22/25	Fri 7/30/32
935	5.1 Development, UAT & Deployment: Release 1.40	92 days	Fri 8/22/25	Fri 1/9/26
948	5.2 Release 1.41 Development, UAT & Deployment	90 days	Mon 1/12/26	Fri 5/15/26
949	5.3 Release 1.42 Development, UAT & Deployment	90 days	Mon 5/18/26	Fri 9/18/26
950	5.4 Release 1.43 Development, UAT & Deployment	85 days	Mon 9/21/26	Fri 1/15/27
951	5.5 Release 1.44 Development, UAT & Deployment	85 days	Mon 1/18/27	Fri 5/14/27
952	5.6 Release 1.45 Development, UAT & Deployment	90 days	Mon 5/17/27	Fri 9/17/27

953	5.7 Release 1.46 Development, UAT & Deployment	85 days	Mon 9/20/27	Fri 1/14/28
954	5.8 Release 1.47 Development, UAT & Deployment	90 days	Mon 1/17/28	Fri 5/19/28
955	5.9 Release 1.48 Development, UAT & Deployment	85 days	Mon 5/22/28	Fri 9/15/28
956	5.10 Release 1.49 Development, UAT & Deployment	90 days	Mon 9/18/28	Fri 1/19/29
957	5.11 Release 1.50 Development, UAT & Deployment	85 days	Mon 1/22/29	Fri 5/18/29
958	5.12 Release 1.51 Development, UAT & Deployment	90 days	Mon 5/21/29	Fri 9/21/29
959	5.13 Release 1.52 Development, UAT & Deployment	85 days	Mon 9/24/29	Fri 1/18/30
960	5.14 Release 1.53 Development, UAT & Deployment	85 days	Mon 1/21/30	Fri 5/17/30
961	5.15 Release 1.54 Development, UAT & Deployment	90 days	Mon 5/20/30	Fri 9/20/30
962	5.16 Release 1.55 Development, UAT & Deployment	85 days	Mon 9/23/30	Fri 1/17/31
963	5.17 Release 1.56 Development, UAT & Deployment	90 days	Mon 1/20/31	Fri 5/23/31
964	5.18 Release 1.57 Development, UAT & Deployment	85 days	Mon 5/26/31	Fri 9/19/31
965	5.19 Completion of Base M&E Contract	225 days	Mon 9/22/31	Fri 7/30/32
966	▷ 6 Transition-Out Phase	85 days	Tue 4/1/31	Thu 7/31/31
973	7 Seven Year Contract Closed	0 days	Thu 7/31/31	Thu 7/31/31
974	▷ 8 Optional Year 8	2149 days	Fri 8/1/25	Wed 3/1/34
986	▷ 9 Optional Year 9	262 days	Fri 7/29/33	Mon 7/31/34
998	▷ 10 Optional Year 10	262 days	Mon 7/31/34	Tue 7/31/35
1009	11 Contract Closed	0 days	Tue 7/31/35	Tue 7/31/35

Figure 4: Draft Project Schedule

The full Microsoft Project file will be kept on SharePoint with exports to Excel or PDF provided as needed.

Appendix D: Quality Assurance Management Plan

The following pages provide NC WIC with the Quality Assurance Management Plan which describes the approach to managing quality for the North Carolina Crossroads Maintenance and Enhancement project.

State of North Carolina
Department of Health and Human Services
Division of Child and Family Well-Being



Crossroads MIS
Maintenance and Enhancement Services

North Carolina WIC Program

Appendix D
Quality Assurance Management Plan

Trademarks

Trademarked names may appear throughout this document. Rather than list the names and entities that own the trademarks or insert a trademark symbol with each mention of the trademarked name, the names are used only for editorial purposes and to the benefit of the trademark owner with no intention of infringing upon that trademark.

Contact Information

To request copies, suggest changes, or submit corrections, contact:

North Carolina Department of Health and Human Services**Division of Child and Family Well-being, WIC Program**

Attention: Molly Jones

Crossroads WIC Release Manager

Phone: 252-903-3951

Email: Molly.Jones@dhhs.nc.gov

Revision History

Date	Version	Revised By	Description
12/18/2018	0.1	Jay Saunders, Three Sigma Software	Draft version
3/6/2025	1.0	Jennifer Saunders, Voyatek	Submission for RFP 30-25002-DCFW

Deliverable Description

This Quality Assurance Management Plan describes the approach to managing quality for the North Carolina Crossroads Maintenance and Enhancement project.

Table of Contents

1	Purpose	1
1.1	Introduction	1
1.2	Scope	1
1.3	QM Guidance	2
2	Quality Management Approach.....	3
2.1	Team Roles and Responsibilities	3
2.2	Quality Status Meeting.....	4
2.3	Quality Register	5
3	Quality Planning	6
4	Quality Assurance.....	8
5	Quality Control	11
6	Quality Improvement	14
7	Process Quality Assurance Management	15
7.1	Deliverable Quality	15
7.2	Service Quality	16
7.3	Software Development Quality Assurance Management	17
7.4	Measure of Quality.....	18
7.5	Quality Management Records and Reports	19
8	Quality Measurements and Tools	20
9	Quality Management Problem Resolution.....	22

Table of Figures

Figure 1: Deliverable Quality Process	15
Figure 2: Service Quality Evaluation	17

Table of Tables

Table 1: Voyatek Project Team Quality Roles and Responsibilities	3
Table 2: Quality Assurance Standards	8
Table 3: Quality Control Standards.....	11
Table 4: Tools, Techniques, and Methodologies by Lifecycle Phase	20

1 Purpose

The purpose of this document is to provide details on a Quality Management (QM) strategy for information technology activities (software, hardware, and services) to be performed in support of the North Carolina WIC. This document provides a basis for planning, performing, managing, monitoring, and measuring Crossroads quality management activities.

This Quality Assurance Management Plan (QAMP) defines the QM principles and the QM activities to be performed during the lifecycle of the NC WIC Maintenance and Enhancement Project. It supplies a systematic method for identifying, tracking, and resolving all quality issues. It also describes the responsibilities and authorities for accomplishing the planned quality management activities and identifies the required coordination of quality management activities with other Project/Program activities.

1.1 Introduction

The QAMP documents how Voyatek and the State will plan, implement, and assess the effectiveness of its quality planning, quality assurance, quality control, and quality improvement activities. The following activities make up the quality system that will be used by the Quality Management Team to manage and support NC WIC Maintenance and Enhancement Project.

Quality Planning (QP): Quality planning is the identification, selection, and creation of quality standards and related procedures relevant to the systems and services being delivered. This includes the application of industry standards (e.g., PMBOK, IEEE) and the definition of the roles and responsibilities of the resources involved in the planning and execution of quality processes. It defines the procedures and tools used to validate and confirm the quality of deliverables.

Quality Assurance (QA): Evaluating overall project performance on a regular basis to provide confidence that the project will satisfy the relevant quality standards established during QP.

Quality Control (QC): Monitoring specific products to ensure they comply with relevant quality standards. It includes the evaluation process, testing activities, and operations techniques involved in monitoring project deliverables to determine whether they comply with relevant quality standards, NC WIC requirements, and agreed-upon specifications.

Quality Improvement (QI): To use output indicators to help identify better standards in order to increase the project's effectiveness and efficiency. Continuous quality improvement is a core component of QM. It defines the process for monitoring and reviewing processes and understanding the extent to which those processes impact the quality of deliverables. This information is then used to make improvements to project activities. The goal of the continuous improvement process is not only to prevent non-conformities from recurring, but also to provide an ongoing elevation of the quality level delivered on the project.

The plan outlines QM activities to be performed in support of the NC WIC. QM activities are an integral part of the processes used to develop and deliver work products and services to the State.

1.2 Scope

The scope of Quality Assurance Management Plan (QAMP) is to provide processes that are required to ensure the quality program implemented will satisfy the delivery of Crossroads system maintenance and enhancement and associated documentation. The overall management determines and implements the quality guidance described in this document, objectives, and responsibilities; implementation is conducted under the mantles of Quality Planning (QP), Quality Assurance (QA), and Quality Control (QC), with the ultimate goal of producing a quality product while

facilitating/fostering Quality Improvement (QI). Avoiding mistakes and reworks will save valuable time, effort, and resources. QM provides the tools, techniques, and methodologies to support every step in the project lifecycle.

This QAMP defines the activities and processes related to managing the quality of the NC WIC system maintenance and enhancement. It is applicable to the software development lifecycle including project management, detailed analysis, business process re-engineering, design, configuration, modification, extension, data conversion, testing, installation, implementation, training, and on-going support of the application.

1.3 QM Guidance

The purpose of this section is to establish guidance for Quality Management (QM) for the NC WIC Program.

1.3.1 The QAMP will specifically identify the products and processes that are subject to QM review and audit.

1.3.2 A QM team will be formed and that group will establish QM standards, practices, policies, conventions, metrics, and tools.

1.3.3 QM will start concurrently with Project Management, and will continue throughout the Project's lifecycle.

1.3.4 The QM team will regularly review products and processes according to a planned schedule, and will collect, maintain, and retain output QM records for the life of the product and process.

1.3.5 The QM team will perform internal product assessments/audits to assess compliance with specifications, standards, NC WIC requirements, or other criteria.

1.3.6 Program management will regularly review quality assurance and quality control activities, and QM status and effectiveness. The Project/Product Management Plan (PMP) will define the events and intervals for this review.

1.3.7 QM will work to foster constructive communications, provide feedback to detect and prevent development problems, control risks, discuss alternative solutions, and ensure quality is built-in to all products and services.

2 Quality Management Approach

The quality management approach for NC WIC will help ensure quality is planned for both the product and processes. In order to be successful, this project will meet its quality objectives by utilizing an integrated quality approach to define quality standards, measure quality and continuously improve quality.

The NC WIC project quality approach involves including stakeholders and quality assurance team members early in the project phases. This will allow the team to focus on items related to quality in the initial stages so that specific quality activities and standards are incorporated earlier in the project. The NC WIC project will also use bi-weekly and Quarterly project quality measurement reports as a tool to communicate any quality risks or issues that arise.

2.1 Team Roles and Responsibilities

Voyatek Project/ Quality Management and every member of our team, regards quality assurance and quality control activities as a shared responsibility and an essential ingredient to the success of the project.

Table 1: Voyatek Project Team Quality Roles and Responsibilities

Quality Roles and Responsibilities	
Voyatek Role	Description of Quality-Related Responsibilities
Company Executive Management	- Establishing a quality program committed to excellence by making staff and other resources available as needed to support QM - Reviewing and Approving the QM Plan. - Ensuring that resolutions and follow-ups on any quality issues raised by QM are enforced. - Work with the product manager to ensure that client quality expectations are met
Product Manager	- Provides management guidance to the QM Team; - Identifies required tasks as needed by QM; and - Ensures that all assigned tasks follow all applicable policies, directives, methods, processes, and practices. - Ensures that the quality control measures and communications are included in the Project Plan - Ensure deliverables meets all applicable Quality Standards, acceptance criteria and requirements
Quality Assurance Team	- Participate in audits. - Coordinate with customers, stakeholders, and program team members in understanding NC WIC policies and procedures. - Support the QMS in developing and implementing ERA policies and procedures. - Communicate with other State Managers, SMEs and other stakeholders who may propose improvements to QM practices

Quality Roles and Responsibilities	
Voyatek Role	Description of Quality-Related Responsibilities
Test Manager	• Ensure testing is conducted per the test plan and other test documentation. • Reviewing and commenting on the QAMP • Implementing the quality program in accordance with this QAMP • Resolving and following-up on any quality issues raised by QM relating to testing activities. • Ensure entry criteria are achieved prior to Acceptance Test start. • Perform Acceptance Testing of the delivered product. • Ensure exit criteria are achieved prior to Acceptance Test signoff. • Implementing the test practices, processes, and procedure as defined in the Test Plan.
Configuration Management (CM) Lead	• Coordinate configuration audit responsibilities with QM. • Implementing the quality program in accordance with this QAMP • Reviewing and commenting on the QAMP • Store records (reviews) and artifacts (audits) generated by QM activities. • Conduct Functional Configuration Audit (FCA) and Physical Configuration Audit (PCA) as per the integrated Schedule. • Ensure CM Audits are conducted on all baselines Implementing the CM practices, processes, and procedures as defined in the CMP.
Release Management Lead	• Informs QM when a production deployment is ready for verification review; • Provides assistance to QM for specific requests from QM for a quality review of a production deployment; • Receives confirmation from QM of deployment reviews and reply to issues found as needed.

2.2 Quality Status Meeting

The QAMT Meeting gives Project leadership and functional area managers an opportunity to understand and participate in the Quality effort. The QMT holds a Quality Status Meeting bi-weekly. The QMT team sends out a status report the day before the event. The Quality Manager chairs the Meeting. Functional area representatives attend the meeting. The report/meeting addresses the following topics:

- Metrics Management
- Problem Management
- Plan/Process Audits
- Document Review Assessments
- QMT and Current Activities/Accomplishments, Completed Activities, and Forecasted Activities
- Summary of Action Items

- Summary of Quality Findings
- Recommended Improvements

2.3 Quality Register

The Quality Register is a diary of the quality events planned and undertaken, such as status reports, deliverable reviews, audits, Findings, Action Items, etc.). The QMT maintains the register throughout the project. As the project progresses and records of the quality activities are acquired, updates to the Quality Register reflect the actual results from the quality activities.

In the subsequent sections of this document, the following quality management approach elements are described and defined:

- Quality Planning, Quality Assurance, and Quality Control
- Quality activities & standards relevant to NC WIC
- Appropriate quality metrics and measures for standards for project processes, product functionality, project deliverables, project management performance, documentation, and testing
- Tools & software used to support quality management
- QA & QC problem reporting and resolution plan

3 Quality Planning

Quality planning is the process of identifying quality requirements and/or standards for the project and product, and documenting how the project will demonstrate compliance. The deliverables and processes to be reviewed for the NC WIC project, and their corresponding quality standards, are detailed in the Quality Assurance and Quality Control sections of this document.

The QAMP will be updated during the Transition – In Phase of the project, and is a parallel activity with other processes through the lifecycle of the project. The intended audience is the Product Manager, Project Team, State and any senior leaders whose support is needed to carry out the plan. Implementation of and compliance with the QAMP, is the shared responsibility of all project personnel. Both project management and technical staff are thus integrated with and committed to the success of overall quality management.

Quality planning also includes establishing the quality standards, identification of the quality metrics to be applied, creating the quality checklists, and conducting problem remediation activities. These processes are described at a high level below:

Establish Quality Standards

This quality planning process establishes the QA & QC standards – the process descriptions, standards, and procedures – the NC WIC Project Team will use. The Product Manager, in collaboration with the Team Leads and Process Owners, have defined and developed the quality process descriptions, standards, and procedures that are applicable to the NC WIC project phases.

Identify Quality Metrics

This quality planning process identifies the metrics the Team will use. The Product Manager, in collaboration with the Team Leads and Process Owners, have identified and developed the quality metrics applicable to the NC WIC project. The metrics, which are based on the quality standards established by the Project Team, will be refined during the different phases of the project, and documented in updates to this Quality Assurance Management Plan. The Project Team will use the quality metrics to evaluate whether the project is achieving its goals.

Create Quality Checklists

This quality planning process identifies the quality checklists the Team will use. The Product Manager, in collaboration with the Team Leads and Process Owners, have defined and developed the quality checklists that are applicable to the NCWIC project. The Project Team will use the quality checklists an integral part of the process and product quality reviews.

The Process Quality Assurance and Product Quality Assurance sections of this plan discuss the application of these checklists to the respective quality assurance processes. These checklists are included in the Product and Process Quality Checklist sections of this document.

Problem Remediation

The Product Manager will schedule separate meetings as needed to determine corrective actions and process improvements. The results of the activities are then acted on, where possible, to improve the success of future project phases by incorporating experiences and lessons learned into subsequent phase planning activities. Through the incorporation of quality management

recommendations from the preceding review stage into the activities and related deliverables for the next stage, the quality of project activities and deliverables will increase incrementally throughout the project life cycle. This approach minimizes issues at the end of the project and facilitates a successful outcome.

4 Quality Assurance

Quality assurance, which is focused on the project processes, provides confidence that the quality requirements can be fulfilled and helps ensure that the project processes used to manage and deliver the project's product or service are effective and being applied. In order to ensure quality, an iterative quality process will be used throughout the project life cycle. This iterative process includes measuring process metrics, analyzing process data, and continuously improving the processes; to identify, assess, respond to, monitor, and control project quality, all NC WIC stakeholders will be involved.

The Product Manager will schedule regularly occurring meetings to review the findings of the quality assurance activities. In these reviews, an agenda item will include a review of project processes, any discrepancies and/or audit findings from the Product Manager or other assigned project team owner, and a discussion on process improvement initiatives. These reviews, findings, and assessments should result in some form of process and/or product improvement. All process improvement efforts must be documented, implemented, and communicated to all team members as changes are made.

The matrix below describes the quality assurance standards for the NC WIC project:

Table 2: Quality Assurance Standards

Project Process	Quality Assurance Process or Activity	Inputs Include:
Project Schedule Management	• Objective: Verification that Project Schedule Management activities are performed via a documented process. • Per the Project Schedule Management Plan: • Project schedule review meetings occur • Project schedule review meetings are well attended • Modifications to the project schedule approved and tracked • Impact estimations occurring outside of/prior to the schedule modification process • Roles and responsibilities are well defined • Action items from review meetings are documented and tracked to completion	• Schedule Management Plan • Project Schedule Standards

Project Process	Quality Assurance Process or Activity	Inputs Include:
Design Review	• Objective: Verification that Design Review activities are performed via a documented process. • Per Design Review standards document: • Design review meetings occur • Design review meetings are well attended • Modifications to the design documents are approved, tracked, and documented appropriately • A process is in place to communicate design changes to the Development and Testing teams • Roles and responsibilities are well defined • Executive review and analysis of design quality, based on checklists, occurs on schedule • Design review processes are implemented to ensure that the design inputs were correctly selected and incorporated	• Design Standards • Design Review Process Document
Change Management	• Objective: Verification that Change Management activities are performed via a documented process. • Per Change Management Plan: • Change Management meetings occur • Meetings are well attended • Agenda created for each meeting and distributed 24 hours prior • Minutes for each meeting posted within 24 hours of meeting end • A process is in place to communicate approved changes to the Development and Testing teams • Roles and responsibilities are well defined	• Change Management Plan • Change Control Board Guidelines • Project Management Plan • Change and Configuration Management Standards and Guidelines

Project Process	Quality Assurance Process or Activity	Inputs Include:
Risk Management	• Objective: Verification that Risk Management activities are performed via a documented process. • Per Risk Management Plan: • Meetings are well attended • Agenda created for each meeting and distributed 24 hours prior • Minutes for each meeting posted within 24 hours of meeting end • Risks & Issues appropriately categorized based on risk level, impact, etc. • Roles and responsibilities are well defined • Risks & Issues are escalated to Senior Management as needed	• Project Management Plan • Risk Management Plan
Peer Review	• Objective: Verification that Peer Review activities are performed via a documented process. • Per Peer Review document: • Peer reviews in place and results are documented • Formal and informal reviews in place	• Development Plan • System Development Standards and Guidelines
Test Management (Software Validation and Verification)	• Objective: Verification that Test Management activities are performed via a documented process. • Per Test Plan: • Test review procedures are well-defined • Rigorous verification approach in place and being used • Test procedures are self-explanatory (can be understood by someone other than the author) • Test results are tracked in the testing tool • Appropriate for degree of software criticality	• Test Standards and Guidelines • Test Plan

Project Process	Quality Assurance Process or Activity	Inputs Include:
Defect Management	• Objective: Verification that Defect Management activities are performed via a documented process. • Per Defect Management processes: • Defect process is being followed per approved defect management plan • Defects are tracked in the Defect Management tool	• Production Support Standards and Guidelines • Test Plan • Defect Management Standards & Guidelines

5 Quality Control

Quality control is focused on the products and deliverables of the project. It is the process of monitoring project deliverables to verify that the deliverables are of acceptable quality and are complete and correct, and includes the inspection, analysis, and actions required to ensure quality output. The NCWIC QC process involves the following steps:

- Verifying, validating, and monitoring of work products to ensure the requirements for quality and scope of work are being fulfilled
- Inspecting deliverables and documentation and comparing these items to a standard of quality defined by industry standards (e.g., PMBOK, IEEE) and the stakeholders of the project
- Verifying that both the user's requirements and technical specifications are met before and after the work product is approved and is promoted into a stable production environment
- Monitoring output of workflows progress, detecting problems and defects, and allowing for corrections prior to delivery of work products or services

The Product Manager will schedule regularly occurring project, management, and document reviews. In these reviews, an agenda item will include a review of products, any discrepancies and/or audit findings from the quality manager/quality reviewer, and a discussion on product improvement initiatives.

The matrix below describes the quality control standards for the NC WIC project:

Table 3: Quality Control Standards

Project Product	Quality Control Standards	Inputs Include:
Project Schedule Inspection	• Resource allocations do not exceed 100% • Plan is baselined • All tasks (excluding summary & milestone) have resources assigned • All project phases realistically represented	• Project Plan Document • Project Schedule Standards

Project Product	Quality Control Standards	Inputs Include:
Change Management Documentation Review	• CCB minutes are updated weekly with next actions, owners, and due dates • Change Orders are properly documented and contain all necessary impact assessments and approvals • Approved change orders are reflected in the schedule	• Change Management Plan • Change Control Board Guidelines • Project Management Plan • Change and Configuration Management Standards and Guidelines
Risk & Issue Management Documentation Review	• Risks & Issues are properly documented in the tracking tool • Risks & Issues not open greater than 30 days • Risks & Issues properly categorized	• Project Management Plan • Risk Management Plan
Requirements Traceability Matrix audit	• User requirements are traced to software requirements • Requirements uniquely identified and traced to design document(s)	• Design Standards & Guidelines • Requirements Management Plan
Test Plan & Use Case Review/Inspection	• Review post-test execution related artifacts including test reports, test results, problem reports, updated requirements verification matrices, etc. • Integration test design exists for every interface • Unit test plan defines coverage requirements • System test design for each software component • Realistic testing & repair work estimates in project schedule	• Test Standards and Guidelines • Test Plan
Design Document Inspection	• Proper template used to create the design • Approvals obtained and documented in the design or a corresponding document • Design free of spelling and grammar errors	• Design Standards & Guidelines

Project Product	Quality Control Standards	Inputs Include:
Defect Inspection	• Failed tests are repeated after correction • Defect triage process in use and effective • Defects are categorized per the plan (type, cause, module) • Test anomalies are identified, documented, addressed, and tracked to closure	• Production Support Standards and Guidelines • Test Plan • Defect Management Standards & Guidelines

6 Quality Improvement

The Process Improvement Reviews lend support to the whole QM concept in that they are held to evaluate metrics from the development effort. Process Improvement is successful when an effective process emerges or evolves that can be characterized as: practical, documented, enforced, trained, measured and improvable. Their findings provide information needed to determine if processes need to be modified to prevent or reduce quality related problems in the future of the Project/Program or in new efforts. This type of review generates process improvement recommendations.

7 Process Quality Assurance Management

Process quality assurance management focuses on the processes required for the NC WIC Project, how these processes are implemented, and how they are monitored. One of the critical objectives for ensuring that quality deliverables and work products are produced is ensuring that all team members are aware of, and rigorously adhere to, the established quality standards and management processes. Therefore, in addition to providing the framework for monitoring specific project deliverables and work products, the QM process also provides the construct for validating that the project team adheres to all project management processes quality standards.

Quality Management includes two main components, Deliverable Quality and Service Quality processes. To achieve a positive outcome, these processes will be carried out so expectations are aligned and met.

7.1 Deliverable Quality

The diagram below depicts the Deliverable Quality process. Each yellow star indicates a quality management element. These elements are described in more detail below.

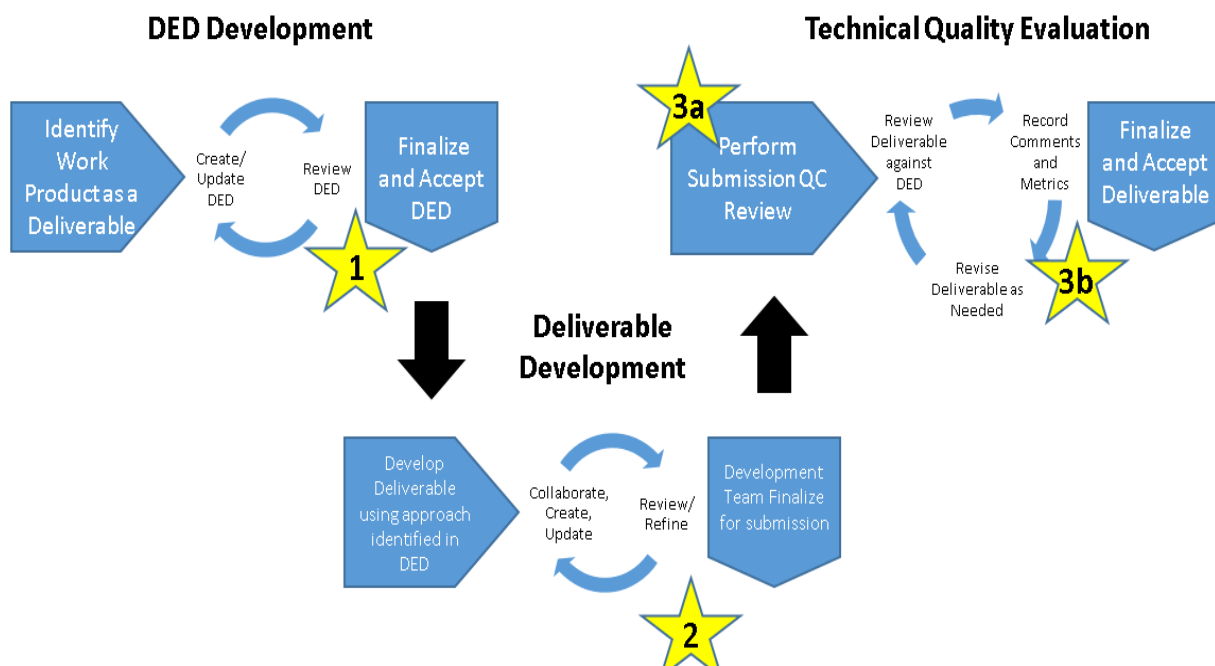


Figure 1: Deliverable Quality Process

Voyatek Deliverable Quality Management process has elements designed into each of the three key stages of a Deliverable; these elements are as follows:

1. Deliverable Expectation Document (DED) Development - The DED is the first step in establishing the quality expectations for the deliverable before deliverable development begins. It establishes the criteria and format by which the eventual deliverable submission will be measured. Through the review and acceptance of the DED, the impacted stakeholders

collaborate to set clear expectations and agree upon outcomes as well as communicating the approach for developing and accepting the content in parts or in its entirety.

2. Deliverable Development – Voyatek encourages coordination and collaboration throughout the development of a deliverable. The deliverable Owner establishes quality checkpoints to confirm acceptance criteria, and the approach to be used for the development of a deliverable. For Contractual deliverables, the Product Manager ensures that the deliverable Owner uses Check Lists to confirm that quality expectations have been included in the deliverable.
3. Technical Quality Evaluation
 - a. Submission QC Review – The first step in the Technical Quality Evaluation process is to review the deliverable against a standard checklist to confirm it meets the Project’s quality standards prior to the deliverable review process. If any issues are found, the submission is not accepted and the deliverable is returned to the Owner. This step helps ensure the most efficient use of the Reviewers’ time and provides a clear indicator of the quality to the deliverable Owner.
 - b. Deliverable Review – The quality component during the deliverable review process confirms accuracy and completeness meets the deliverable acceptance criteria communicated in the DED.

7.2 Service Quality

The purpose and scope of Service Quality is focused on the overall interactions and performance of the service provider/vendor (Voyatek) during a specific period of time. Service Quality Management and Procedures, in conjunction with the Deliverable Quality, Schedule, and Deliverable Management, will provide a complete view of a performance. Voyatek’s performance will be monitored and evaluated.

The process for evaluating Voyatek’s service quality is illustrated in the diagram shown below. It consists of the following:

- Initial Meeting - During the Transition-In Phase Voyatek Project and Quality Managers and Engagement Executives, will meet with NC WIC to confirm contractual and service level expectations for the Project
- Service Quality Evaluation - Service Quality evaluators may utilize the Service Quality questionnaire and Checklists to gather and analyze feedbacks.
- Final Evolution Reviews - At the end of the project Quality Evaluation and feedback sessions will be held as part of project closure. The purpose of these sessions is to review the overall quality performance for the engagement.



Figure 2: Service Quality Evaluation

7.3 Software Development Quality Assurance Management

Voyatek is heavily focused on software development quality assurance, in order to monitor systems development efforts and ensure that the appropriate standards and processes are maintained. For the maintenance and enhancement of Crossroads, Voyatek development staff has online access to the policies and processes for system design, documentation, configuration, and record management.

Version control and audit capability support comprehensive documentation of each base component and subsequent changes as they occur. The most current system documentation is always identifiable, while historical versions are also available for reference. A project repository of project and system documentation will be setup and made accessible to all authorized members of the project team.

Our software development process is a mature, repeatable process that yields high quality software. The benefit of this to NC WIC is not just high quality results but also predictability—a key factor in the maintenance and enhancement of large-scale systems such as Crossroads.

Software Quality Assurance (SQA) Approach

SQA methods include testing, inspection, formal methods (such as program verification and model checking), static code analysis (also called non-executable based testing), and runtime verification (also called executable based testing). A disciplined approach to SQA ensures a higher level of quality in the final product, resulting in reduced implementation costs, increased satisfaction in the final product, and a significantly higher return on investment for NC WIC

Pre-Development

The purpose of software quality assurance is to find both predictive and undefined faults. Early and regular quality-related activities reduce the number and seriousness of faults encountered during the software development process. It is not possible to arrive at high quality software just by testing and debugging the software. Quality must be integrated into all phases of the system development lifecycle—from the beginning of requirements analysis effort to final testing. To facilitate this, software testing is done during the early stages of system development as well as during the

development and integration cycles. Testing of the requirements definition, analysis, and design efforts are of primary importance in the early stages of development. This is done by reviewing and verifying processes and documentation produced by the activities listed above.

Use Case serves as the basis and starting point for all software testing. For this effort, the use case descriptions captured in the requirements specification are used to facilitate testing. When a use case is complete, the test team begins creating test scripts and scenarios. This allows the testing to begin in parallel to the development cycle instead of waiting for a development baseline. The testing team completes formal testing by executing each use case step and alternate course and documenting a pass/fail result.

Frequent Testing Throughout the Development Cycle

Testing at each level of the development cycle is critical in the development of quality software. To ensure high quality products we apply a comprehensive and disciplined test methodology that includes careful upfront planning to ensure thorough testing. Our quality assurance testing methodology is based on a “bottom-up” test philosophy, which allows for forward-moving baselines to enable sets of use cases to be tested in an iterative fashion to find and resolve faults as early as possible. At each stage, software is defined with greater precision until it becomes actual operating software. At certain stages, the definition of the software reaches a degree of stability that is sufficient for review and acceptance by the test organization. A baseline, therefore, represents a point in the process where a certain scope of software is defined well enough for the pertinent stakeholders in the project to objectively accept that definition.

Our quality assurance processes are responsible for validating requirements, reviewing test cases, and ensuring the input of the conditions necessary to test all necessary conditions. Furthermore, the testing team verifies the execution of the scripts and collects tests results for evaluation and reporting. We track all defects and monitor testing results throughout the software development cycle; and provide feedback to the development team to improve the quality of the software under development.

7.4 Measure of Quality

Voyatek’s Process Quality Management approach includes a metrics program whereby key project metrics are tracked and reported on throughout the project. The information gathered from the metrics program is used to analyze many aspects of the project, including software development quality, and provides project managers with the information necessary to make informed management decisions for the project.

During Transition-In Phase, the Voyatek Product Manager works closely with the NC WIC managers to develop the specific details of the metrics program. This includes identifying the metrics to be used over the life of the project, including those measures that relate to software quality assurance. Some of these indicators may include:

Software Quality Index (SQI). A weighted metric indicating the number and severity of defects. This is a metric indicating the relative quality of the software.

Number of Defects Over Time. A metric indicating the occurrence of defects over time during development. Decreasing numbers of defects is an indicator of improvement in the overall software application being developed.

Number of Defects Closed Over Time. A metric indicating the number of defects successfully resolved during project development. An increasing number of closed defects are indicative of improvement in the quality of the software.

Total Open Defects. A metric indicating the current unweighted number of open defects. Declining numbers indicate progress in eliminating defects.

The preceding metrics are illustrative of those that could be used to track the quality of performance for Crossroads.

7.5 Quality Management Records and Reports

The NC WIC Project team will maintain records that document assessments performed on the project. Maintaining these records will provide objective evidence and traceability of assessments performed throughout the project's life cycle. Example records include the process and product assessments reports, completed checklists, metrics, and weekly/monthly status reports. The project team will use a shared document repository to contain the reporting data and the reports produced as part of the quality activities and reviews. The records will be maintained through the implementation phase of the project.

8 Quality Measurements and Tools

The NC WIC products and processes identified in the quality planning sections of this document must be measured and should fall within the established standards and tolerances. When QC measurements do not meet the agreed-upon quality levels, the Voyatek Product Manager and the State will define the action steps for the discrepancies. Actions may vary depending on the process or the deliverable being inspected or reviewed.

The NC WIC team may use many different tools when performing quality management activities for the project. Samples of potential tools are listed below:

Software Quality Tools

- Microsoft Office Tools (i.e., Project, Word, Excel, and PowerPoint)
- Defect Management Repository & Defect Tracking Software
- Test Management Software
- Test Management Repository

This table below identifies the tools, techniques, and methodologies to be used to support QM for a given Lifecycle Phase.

Table 4: Tools, Techniques, and Methodologies by Lifecycle Phase

Lifecycle Phase	Tools	Techniques	Methodologies
Requirements & Design	• Microsoft Access • Microsoft Excel • Microsoft Word • SharePoint • TFS	• Peer Reviews • Walkthroughs • Audits • Problem/ Deviation Reporting	• Action Item Form • Change Request/Proposal Form • Peer Review Action Item Tracking System Database Users Guide • Peer Review Action Item Log Form • Assessment/Audit Checklist and Report

Lifecycle Phase	Tools	Techniques	Methodologies
Implementation & Test	• Microsoft Access • Microsoft Excel • Microsoft Word • SharePoint • TFS	• Peer Reviews • Walkthroughs • Audits • Problem/ Deviation Reporting	• Action Item Form • Change Request/Proposal Form Peer Review Action Item Tracking System Database Users Guide • Peer Review Action Item Log Form • Assessment/Audit Checklist and Report
Installation & Checkout	• Microsoft Word • SharePoint • TFS	• Audits • Problem/ Deviation Reporting	• Action Item Form • Change Request/Proposal Form • Assessment/Audit Checklist and Report
Operations & Support	• Microsoft Word • SharePoint • TFS	• Audits • Problem/ Deviation Reporting	• Action Item Form • Change Request/Proposal Form • Assessment/Audit Checklist and Report

9 Quality Management Problem Resolution

The NC WIC Product Manager will monitor quality and report exceptions to the State as part of monthly status reporting, or more frequently if conditions warrant.

The QA & QC activities will occur on a monthly basis, and may be measured monthly or bi-weekly depending on the approved schedule. For each review, the reviewer will complete the QA/QC logs. Within one week of review, the results of the quality activities will be reviewed with the Process Owner/Manager for that specific activity. During this review, the Product Manager, and the Quality Reviewer will document the plan for resolving the quality issues detailed in the Activity Report. The Product Manager is responsible for the consolidation of the review results into a monthly report that is provided to the State.

The Quality Assurance and Quality Control logs will be used to itemize, document and track to closure items reported through quality management activities. Aged quality issues (>30 days since creation) will be escalated to the Product Manager for response and resolution. The Product Manager may escalate to senior company management, as necessary.

Appendix E: Rehosting Implementation and Rollout Plan

The following pages provide NC WIC with the Rehosting Implementation and Rollout Plan which describes the detailed tasks, process, and schedule for transitioning the hosting of Crossroads from the state data center to the Azure cloud.



Crossroads MIS
Maintenance and Enhancement Services

North Carolina WIC Program

Appendix E
Rehosting Implementation and
Rollout Plan

Trademarks

Trademarked names may appear throughout this document. Rather than list the names and entities that own the trademarks or insert a trademark symbol with each mention of the trademarked name, the names are used only for editorial purposes and to the benefit of the trademark owner with no intention of infringing upon that trademark.

Contact Information

To request copies, suggest changes, or submit corrections, contact:

North Carolina Department of Health and Human Services**Division of Child and Family Well-being, WIC Program**

Attention: Molly Jones

Crossroads WIC Release Manager

Phone: 252-903-3951

Email: Molly.Jones@dhhs.nc.gov

Revision History

Date	Version	Revised By	Description
12/18/2018	0.1	Jay Saunders, Three Sigma Software	Draft version
3/6/2025	1.0	Jennifer Saunders, Voyatek	Submission for RFP 30-25002-DCFW

Deliverable Description

This Rehosting Implementation and Rollout Plan describes Voyatek’s approach to rehosting the NC Crossroads environments from the NC data center to Voyatek’s managed cloud infrastructure.

Table of Contents

1. Introduction	1
2. Roles and Responsibilities	2
3. Planning and Schedule.....	3
4. Implementation Approach	5
4.1 Infrastructure and Services	5
4.2 Deployment Automation.....	6
5. Target Azure Environment Overview	7
6. Security and Network Architecture	8
6.1 Security.....	8
6.2 Security Management	8
6.3 Application Authentication.....	8
6.4 Load Balancing and Firewall Configuration	8
6.5 URL Configuration and Certificates	9
7. Application Configuration and Setup.....	10
8. Infrastructure Monitoring	11
9. Data Migration Strategy	12
10. Rollout and Implementation	13
10.1 Detailed Migration Task Schedule	13

Table of Tables

Table 1: Roles and Responsibilities	2
Table 2: Detailed Migration Task Schedule	13

1. Introduction

The Rehosting Implementation and Rollout Plan outlines the strategy and technical approach for migrating the Crossroads environments that are currently located in an on-premises North Carolina datacenter to a Voyatek managed Azure tenant. The plan will address the migration of the following environments.

1. UAT
2. Staging
3. Sandbox
4. Production
5. Disaster Recovery

The rehosting plan focuses on migrating existing workloads to the Azure East US Commercial Cloud using a strategic combination of Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS) solutions. This approach facilitates a lift-and-shift migration for the web and application tiers, while leveraging Azure-native services for databases, storage, and networking to enhance performance, scalability, and manageability. The choice of East US ensures low latency and cost-efficiency for users on the east coast such as North Carolina WIC, with the option to implement disaster recovery using a different, geographically distant region as a failover/disaster recovery location. This approach accelerates cloud adoption while maintaining compliance with industry standards and governance policies.

2. Roles and Responsibilities

The following table lists the roles and responsibilities for the high-level tasks involved in this effort.

Table 1: Roles and Responsibilities

Task	Description	Responsible Party
1. Assessment & Planning	Review current infrastructure, identify workloads, and confirm migration scope.	Voyatek & NC DIT Team
2. VM Inventory & Dependencies	List all VMs and their dependencies to ensure compatibility with Azure services.	Voyatek & NC DIT Team
3. Design Azure Architecture	Define architecture for VMs, networking, and storage in Azure.	Voyatek
4. Set Up Azure Environment	Prepare Azure resources (virtual networks, storage, security settings).	Voyatek
5. Migrate VMs to Azure	Move virtual machines to Azure, ensuring configurations match target architecture.	Voyatek
6. Database Assessment & Design	Review current database environment and design a solution for migration to Azure.	Voyatek & NC DIT
7. Migrate Databases to Azure	Migrate databases (e.g., SQL Server) to a managed Azure SQL instance or equivalent.	Voyatek
8. Testing & Validation	Perform functional and performance testing to ensure proper migration and functionality.	Voyatek & NC WIC
9. Final Cutover & Go Live	Transition the system to production, ensuring all services are running in Azure and URLs are remapped	Voyatek & NC DIT Team
10. Post-Migration Support	Provide ongoing support to resolve any issues after the migration.	Voyatek

3. Planning and Schedule

Voyatek acknowledges that NC has requested that the hosting environment migration be completed within the eight-month transition-in period. However, Voyatek proposes completion of the transition in four (4) months with a final cutover date mutually agreed upon with NC WIC.

Voyatek acknowledges the information received in Q&A regarding server sizing and will work closely with NC DIT through a series of meetings during the first month (Month 1) of transition-in to document and understand the current UAT, production, and disaster recovery (DR) environments. Although Voyatek has supported the project for the past five years and is familiar with the production environment, these meetings are essential to ensure no details are overlooked during the transition, particularly because Voyatek does not manage these environments. This process will involve reviewing existing infrastructure, capturing detailed configurations, and identifying any dependencies or constraints that may impact the transition. These discussions will create a comprehensive understanding of the current state.

Following this initial assessment, over the next two months (Month 2 and Month 3), Voyatek will develop and submit a detailed architecture plan and updated hosting security plan for the target environment. These plans will outline the proposed infrastructure, security controls, scalability considerations, and compliance with relevant standards and policies. Throughout this phase, Voyatek will collaborate with NC DIT to address any concerns, incorporate feedback, and refine the plans to align with operational and security requirements.

Voyatek will begin building the UAT environment in Month 2 while finalizing the planning documentation. Once the infrastructure and application deployments in UAT have been thoroughly tested and verified, Voyatek will seek final approval for the architecture and security documentation. Any necessary updates to the UAT environment will be made based on feedback from the State's review of this documentation. Upon final approval, Voyatek will proceed with provisioning the production and DR environments to meet redundancy and failover requirements. This work is expected to be completed by the end of Month 3.

Month 4 of the transition phase will be dedicated to State verification, allowing the State to conduct a complete review and validation of the newly provisioned environments. During this period, Voyatek will finalize and update any infrastructure-related project documentation to reflect the end-state system.

Upon receiving State approval, Voyatek will coordinate with WIC and NC DIT stakeholders to establish a final cutover date. This will include final readiness assessments and go-live planning for a smooth transition minimizing disruption to clinic operations.

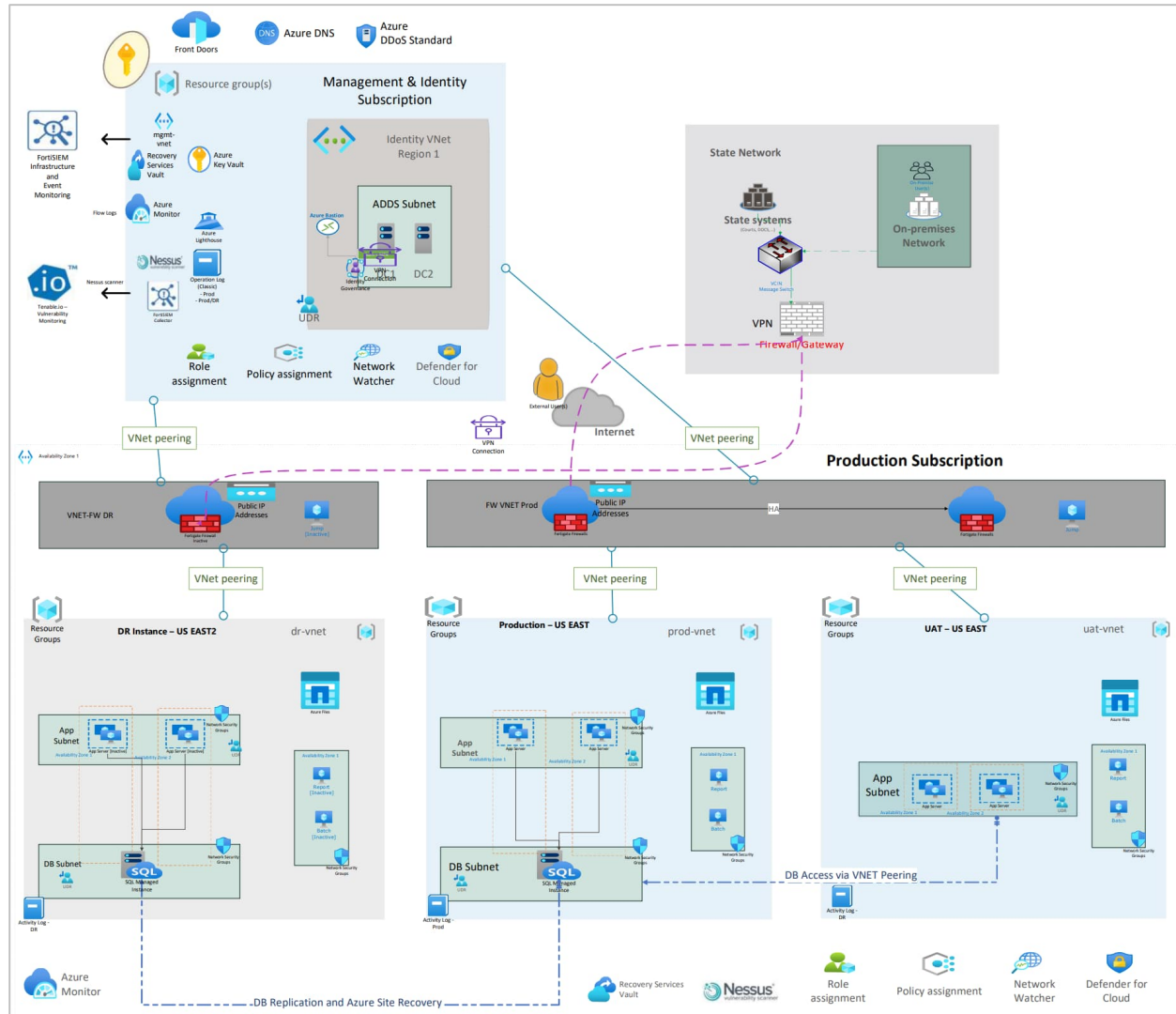


Figure 1- Sample Crossroads Hosting Architecture

4. Implementation Approach

When migrating from on-premises to Azure, especially with a mix of lift-and-shift virtual machines (VMs) and Platform-as-a-Service (PaaS) solutions like Azure SQL, it is often more advantageous to build fresh environments rather than rely on the Azure Migration Tool. While the tool can simplify VM replication, it also brings over legacy configurations, technical debt, and inefficiencies from the existing on-premises setup. By opting for a fresh deployment, we will build an optimized, secure and scalable cloud environment that is fully aligned with Azure’s best practices for performance and long-term success.

Key advantages of Voyatek’s approach are:

1. The ability to design a modern networking architecture with enhanced security, segmentation, and seamless integration through Azure Virtual Network (VNet).
2. Streamlined identity management using Azure Active Directory (AAD) for role-based access control (RBAC), single sign-on, and enhanced security.
3. Full adoption of Azure-native storage and database services, such as Azure SQL and managed storage, to optimize performance and reduce infrastructure overhead.
4. Built-in scalability and automation using Infrastructure-as-Code (IaC) with tools such as Terraform, making deployments more efficient and repeatable.
5. Simplified operations by leaving behind outdated configurations and unnecessary dependencies, resulting in a cleaner, more maintainable cloud environment.

Voyatek’s approach is to simplify the hosting environment by taking advantage of native Azure services wherever possible utilizing automation to deploy both the infrastructure environments and the application using industry standard automation tools. This strategy not only ensures long-term flexibility and cost efficiency but also sets the foundation for future modernization and innovation within Azure.

4.1 Infrastructure and Services

This section outlines the infrastructure and services that will support the Crossroads application within the Azure cloud environment. The architecture is designed to ensure high availability, scalability, and security, and will leverage a combination of virtual machines, managed services, and cloud-native tools. By strategically selecting and configuring services, we aim to provide a robust and reliable environment that meets the application’s requirements and optimizes performance and manageability.

- The Crossroads application components will be hosted on Microsoft Windows Server 2022 virtual machines (VMs). These VMs will be segregated into a secure sub-network on the cloud platform so that access can be strictly controlled. VMs will be deployed to different availability zones to ensure high availability.
- Load balancing/traffic ingress is controlled via a load balancer/application firewall (FortiGate Firewall). All traffic-management components will be configured to be highly available.
- The database will be hosted by a managed instance of SQL Server as a service. This is a Microsoft managed cluster of SQL Server instances that provides better reliability and high

availability. The platform manages failover across availability zones as well as automated backups (and recovery, if needed).

- Azure Storage will be used for storing documents and signature capture files. This service is highly available, with redundant geo-replicated storage.
- Azure DevOps will be used for storing source code and building application components for publishing and deployment.
- Because cloud environments have a flattened structure, we propose unifying the application and web servers to a single tier. This simplifies deployments and eliminates a significant amount of infrastructure, including servers (including reverse proxies) and load balancers.

4.2 Deployment Automation

Voyatek will utilize Terraform to support infrastructure as code which allows us to establish new hosting environments faster with higher reliability and the following advantages:

- Easily set up new environments
- Consistent system environments (development, test, UAT, etc.)
- Stringent source control because changes are tracked, compared, and linked to a specific user
- Changes made outside the automated process are flagged for inspection to ensure the environment(s) are working correctly
- Promotes collaboration on system architecture between developers and operations

From a cloud hosting perspective, this maintains a uniform environment that is deployed according to specification. In addition, having an automated process for deployment helps to eliminate configuration drift for both the infrastructure and deployment settings for each environment being provisioned. Terraform is used to validate that the infrastructure conforms to the baseline specification and Octopus fully deploys the system each time a deployment is completed, which sets any configuration values back to their known baseline.

Octopus Deploy will be used for securely deploying application code to servers in each environment.

5. Target Azure Environment Overview

Voyatek will establish cloud environments for Crossroads to mirror the environments that currently exist on premises. The following section lists the components that will be provisioned in this new environment.

- Shared Components
 - o Virtual networks and subnets for cloud environment management/administration, networking components (like firewalls and load balancers), application components (virtual machines), storage, and database
 - o Network security group rules for basic traffic management between subnets
 - o Firewalls and load balancers for managing inbound traffic to application components (using FortiGate)
 - o Network gateways for outbound traffic
 - o Public IP addresses
 - o Bastion/remote desktop access (using Azure Bastion)
 - o Server monitoring/logging (using FortiSIEM)
 - o Automated deployment infrastructure (using Octopus Deploy)
- UAT and other Pre-Prod Environment Components
 - o With the exception of Octopus Deploy, the base infrastructure components listed above are separate and distinct between pre-production and production environments
 - o Application servers
 - o SQL Server database environment
 - o Storage (using Azure Storage)
- Production Environment Components
 - o Shared components listed above are separate and distinct for pre-production and production environments
 - o Application servers
 - o SQL Server database environment
 - o Storage (using Azure Storage)
- DR Environment Components
 - o Virtual networks and subnets for cloud environment management/administration, networking components (like firewalls and load balancers), application components (virtual machines), storage, and database
 - o Network security group rules for basic traffic management between subnets
 - o Firewalls and load balancers for managing inbound traffic to application components (using FortiGate)
 - o Network gateways for outbound traffic
 - o Public IP addresses
 - o Bastion/remote desktop access (using Azure Bastion)
 - o Reservations for compute resources (VMs)

Voytek will determine server sizing after the detailed planning meetings with NC DIT have been concluded.

6. Security and Network Architecture

6.1 Security

Because we have designed a standard deployment architecture for Crossroads, the security procedures for system usage and access can also be standardized. This process starts with the fundamental networking and access rules between different components. We use Terraform for cloud infrastructure deployment. It encodes network and access rules into a form that can be executed and deployed to the Azure platform. Terraform pushes system components to the cloud environment instead of by hand. The networks that support the system are segregated and inter-network communication configuration only allows known traffic. Virtual machines are hardened by default, with non-essential services disabled. This is done by using pre-made images for the VMs.

6.2 Security Management

Administrative access to the Azure environment and to the VMs, that comprise the system, is strictly controlled.

- Multi-factor authentication (MFA) is required for administrative accounts that have permissions in the Azure portal to configure cloud services
- Access policies for Azure are handled through groups and role assignments at the group level, facilitating effective account management
- Servers are integrated with Azure Active Directory (Entra) to centralize sign-on and allow for user management, including account disablement, to be handled in one place.
- Servers are configured so that logs and access records can be viewed in a single location, separate from the system
- Access to VMs and database is provided only via a “jump box,” a VM configured to allow remote access to the operating environment. The jump box is accessed via the Azure Bastion service, which is integrated with Azure Active Directory/Entra.

6.3 Application Authentication

The Crossroads portals will continue to use NCID Simeio SAML for authentication. TLS will be used end-to-end to secure NCID web service calls. TLS encryption is used for all SAML message exchanges. The Crossroads application uses a service-based API to authenticate against NCID. Voyatek acknowledges North Carolina's intent to integrate the authentication process for Crossroads with Simeio.

6.4 Load Balancing and Firewall Configuration

The system will have several firewalls protecting system components. First, the network on which all the compute and database resources reside is a private network; it is not exposed to the internet. Each subnet within the network will be configured with network security groups that control ingress and egress traffic. Ingress traffic (from the internet, to support the clinic application and web portals) will be routed through a FortiGate device that includes a web application firewall that actively looks for threats. For example, these devices can disallow traffic from outside the United States or look for attack patterns across many requests. They are configured to block malicious traffic, not just ports and protocols.

Calls to external systems will be routed through a network gateway so that servers do not connect to the internet directly. This includes calls to the EBT provider and to other systems like CNDs.

6.5 URL Configuration and Certificates

Both the pre-prod and production environments can continue to use the existing domain (i.e., ncdhhs.gov) and subdomains (e.g., <https://crossroads-wic.ncdhhs.gov> or <https://vendor-wic.ncdhhs.gov>). This would minimize the impact to end users. This would require changes to the IP addresses, and we would need to work with NC DIT to determine whether the certificates would be transferred to the new environments or if new certificates would be procured, and whether the state or Voyatek would own the new certificates.

If North Carolina prefers to use a new domain name for the Voyatek hosted environments, Voyatek will work with the state to determine who would own and procure the new domain name. Voyatek will create subdomains from this to support Crossroads deployments. This would require clinics to change the URL that end users use to access the system.

7. Application Configuration and Setup

The Crossroads application configuration management details are documented in [Configuration Management and Release Management Plan \(Appendix J\)](#). As part of the deployment process, Voyatek will follow the steps outlined under “IIS Configuration” in the section *Crossroads Application Installation and Configuration* to properly configure the IIS infrastructure. This setup is essential for Crossroads to function correctly and will be performed after the underlying servers have been provisioned using Terraform. This is the only manual step in the setup process.

Once the IIS configuration is complete, the next phase involves deploying the Crossroads application using Octopus. Before deployment, Voyatek will install and configure Octopus Tentacles on the Azure virtual machines (VMs) to facilitate automated deployments. These Tentacles will be connected to the production Octopus tenant, enabling centralized management of the deployment process.

Following the Tentacle installation, Voyatek will update the Octopus server configuration to ensure that deployment targets are correctly mapped to the new Azure VMs. This step is crucial to ensuring that future application deployments occur seamlessly in the intended environment.

Once the configuration updates are completed, Voyatek will conduct deployment testing in the User Acceptance Testing (UAT) environment. This process includes verifying that all IIS settings, application components, and dependencies function as expected. Any necessary adjustments or fixes will be made at this stage to resolve potential issues before proceeding to production.

After a successful UAT test, Voyatek will apply the same configuration updates to the production environment. The final step will involve deploying the Crossroads application to the production servers, ensuring a stable and operational set-up. Post-deployment validation and monitoring will be conducted to confirm the system is functioning as intended.

8. Infrastructure Monitoring

The Voyatek Managed Services Network Operations Center (NOC) delivers continuous, real-time monitoring of infrastructure performance with a strong focus on security and availability. Operating 24/7, the NOC leverages advanced remote diagnostic tools and automated threat detection to maintain stability and security of production environments. Voyatek utilizes FortiSIEM extensively on all production environments hosted by our Managed Services organization. FortiSIEM is a top tier security operations center (SOC) and network operations center (NOC) application provided by the security company Fortinet that combines feature sets of both Network Monitoring Products and Security Information and Event Management (SIEM) products.

To maintain a robust security posture, the NOC employs a proactive approach to threat detection and risk mitigation. Security is reinforced through proactive log analysis, traffic inspection, and authentication event monitoring. FortiSIEM enhances these capabilities by collecting and correlating logs from virtual machines (VMs) hosted in the Azure cloud. To achieve this, a FortiSIEM agent will be installed on each Azure VM enabling direct log collection, performance monitoring, and security event detection at the host level. This provides deep visibility into system activity, including application performance, access attempts, and potential threats. Additionally, FortiSIEM integrates with Azure Monitor and Azure Log Analytics to collect security and performance data from managed services, including Azure SQL Managed Instances. Giving the NOC tools and data to monitor database health, query performance, and access patterns to detect potential security risks or performance degradation before they impact operations.

To maintain high availability, the NOC will configure threshold-based alerts for key infrastructure components, including compute resources, network performance, and database operations. The FortiSIEM agent provides near real-time alerting by sending log data directly to the SIEM for correlation and analysis. When anomalies or critical events are detected, automated notifications are generated and sent via email, SMS, or integrated incident management platforms, enabling rapid awareness and response.

In the event of an incident, the NOC will follow structured escalation procedures, leveraging real-time diagnostics and forensic analysis to pinpoint root causes. The integration of host-based monitoring through the FortiSIEM agent, along with cloud-native log collection, enhances incident detection and response, minimizing disruptions while maintaining a secure and highly available infrastructure.

To supplement the native monitoring provided by FortiSIEM, Voyatek has the ability to integrate a third-party monitoring service called Datadog for Application Performance Monitoring (APM). Datadog APM provides an end-to-end visibility into the requests that flow across all the layers of the application enabling efficient troubleshooting and isolating performance issues that might impact end users. Custom monitors and alerting will be configured to proactively notify application developers of potential downstream issues. Datadog provides a wide range of integrations to expand the visibility of resources used in the environment.

9. Data Migration Strategy

Migrating an on-premises SQL Server database to an Azure Managed Instance involves several key steps. The strategy begins with a thorough assessment of the on-premises database, including evaluating its size, dependencies, and compatibility with Azure SQL Managed Instance. The process of migrating the database begins with preparing a full backup of the database. Voyatek will depend on NC DIT to provide this backup. This backup should be created using SQL Server's native backup tools, ensuring that all data, including schema and transaction logs, are captured. Once the backup is complete, NC DIT will securely transfer the backup file from the on-premises environment to Azure via a publicly accessible SFTP (Secure File Transfer Protocol) server site protected by strong authentication credentials. Voyatek will create this SFTP site. Given that no direct connection is available between the current and future environments, this intermediary step is a necessity. The SFTP server acts as a secure repository for the backup file providing a reliable and efficient way to transfer this large file while ensuring data integrity during the move.

Once the backup file reaches the Azure environment, it is stored temporarily in an Azure Storage Blob or a designated file system that is accessible by the Azure Managed Instance. Next Voyatek will restore the database from the backup to the Azure Managed Instance using standard SQL Server restoration processes. The restored database will then be fully operational within the Azure environment with all data and configurations intact. Migration is expected to occur with minimal downtime and data loss because the backup and restore process allows for a near-instantaneous transfer of the database schema and data.

Security is a critical concern in the transfer process. As noted above, there is no direct connection between on-premises and Azure. Using SFTP transmits the backup file securely over an encrypted connection. SSH (Secure Shell) encryption is used to safeguard the file during transit, preventing unauthorized access. Additionally, the SFTP server is configured with robust access controls and authentication mechanisms so that only authorized users can upload or download data. Once the transfer is complete and the database is successfully restored, the backup file will be disposed to prevent risk of exposure. Voyatek will securely delete the backup file from both the Azure Storage Blob and the SFTP server. Furthermore, to minimize the attack surface, the SFTP server will be shut down after migration so that no further access is possible. These steps will be followed so that sensitive data is protected during and after the migration process, preventing unauthorized access and maintaining the confidentiality of the data throughout the entire operation.

10. Rollout and Implementation

The rollout phase represents the critical production cut-over for migrating from an on-premises data center to Azure following a controlled transition. Given the complexity and operational impact of this migration, a detailed and well-structured plan is essential to minimize risks, prevent service disruptions, and maintain business continuity. This section outlines the detailed steps Voyatek will perform over a 48-hour period to transition the crossroads applications to the Azure cloud environment. The table below clearly defines activities, including final system validations, data synchronization, cut-over execution, and post-migration verification, along with the designated responsible party for each task. Each step is carefully coordinated to address dependencies and align teams on execution priorities. By following this structured migration schedule, potential issues will be proactively identified and mitigated, such that the transition to the target environment is smooth and predictable.

An initial version of the Detailed Migration Task Schedule is included in this plan. This ‘living’ schedule will be updated and revised through the transition to capture tasks and responsibilities as they are identified and finalized for the Production transition.

10.1 Detailed Migration Task Schedule

Table 2: Detailed Migration Task Schedule

Date	Time	Responsible	Activity
Day 1 – Friday			
TBD	7:00 PM	NC DIT	Turn off Access to Vendor Portal
TBD	7:00 PM	NC DIT	Turn off Access to Crossroads Application
TBD	7:15 PM	Voyatek/NC WIC	Verify Access to NC DIT Crossroads has been turned off
TBD	7:15 PM	Voyatek/NC WIC	Verify Access to NC DIT Vendor Portal has been turned off
TBD	8:00 PM	NC DIT	Production Database Backup
TBD	8:00 PM	NC DIT	sFTP production DB backup to Voyatek
TBD	8:30 PM	Voyatek	Voyatek DBA restores database to Production NC Environment
TBD	8:30 PM	Voyatek	Verify Batch Services have been updated
TBD	9:00 PM	Voyatek	Verify Restoration of DB is complete with no errors
TBD	9:15 PM	Voyatek	Confirm Encryption Password script has been executed.

Date	Time	Responsible	Activity
TBD	9:15 PM	Voyatek	Voyatek Push Current Production release to NC Production
TBD	9:30 PM	Voyatek	Verify Batch File Control Numbers
TBD	9:30 PM	Voyatek	Confirm sFTP Credentials are entered in Crossroads
TBD	9:30 PM	Voyatek	Confirm Encryption Password script has been executed.
TBD	9:45 PM	Voyatek	Verify Crossroads web service link to CDP/WIC Direct
TBD	9:45 PM	Voyatek	Verify Database Scripts have been run against Production Restore
TBD	9:50 PM	Voyatek	Verify the Batch Service is Running on the Prod Batch server after Deployment of latest version
TBD	10:00 PM	Voyatek	Verify Production code is working - Crossroads App
TBD	10:00 PM	Voyatek	Verify Production code is working - Vendor Portal
TBD	10:00 PM	Voyatek	Verify Production code is working – MyNCWIC Portal
Day 2 - Saturday			
TBD	9:00 AM	Voyatek	Verify Batch process ran correctly for Friday's files
TBD	9:00 AM	Voyatek	Smoke test of NC Production Crossroads App
TBD	9:00 AM	Voyatek	Smoke test of NC Production Vendor Portal
TBD	9:00 AM	Voyatek	Smoke test of NC Production MyNCWIC Portal
TBD	9:00 AM	Voyatek	Verify connectivity with CDP/WIC Direct via Crossroads app
TBD	11:00 AM	Voyatek	Complete Smoke Test Crossroads Application
TBD	11:00 AM	Voyatek	Complete Smoke Test Vendor Portal
TBD	11:00 AM	Voyatek	Complete Smoke Test MyNCWIC Portal

Date	Time	Responsible	Activity
TBD	11:00 AM	NC WIC	Verify connectivity with CDP/WIC Direct via Crossroads app
TBD	11:00 AM	Voyatek	Turn Crossroads app over to NC for testing
TBD	11:00 AM	Voyatek	Turn Vendor Portal over to NC for testing
TBD	11:00 AM	Voyatek	Turn MyNCWIC Portal over to NC for testing
TBD	1:00 PM	NC WIC	Complete Smoke test of Crossroads Application
TBD	1:00 PM	NC WIC	Complete Smoke test of Vendor Portal
TBD	1:00 PM	NC WIC	Complete Smoke test of MyNCWIC Portal
TBD	2:00 PM	Voyatek/NC WIC	Verify Access to Crossroads Production app For NC Clinic Staff
TBD	2:00 PM	Voyatek/NC WIC	Verify Access to Vendor Portal for NC Vendors
TBS	2:00 PM	Voyatek/NCWIC	Verify Access to MyNCWIC Portal for NC Participants
Day 3 - Sunday			
TBD	9:00 AM	Voyatek	Outstanding Issue(s) Resolution

Appendix F: Disaster Recovery and Contingency Plan

The Disaster Recovery and Contingency Plan provides a framework for addressing potential disaster scenarios that could impact the North Carolina Child and Adult Care Food Program (CACFP) system. This document details the procedures for managing disaster recovery efforts affecting Voyatek facilities or operations, as well as the support provided during such events that impact North Carolina facilities or operations. It includes guidelines for declaring a disaster, communicating with state staff, maintaining interim business operations, and the steps required to restore full operational capacity.

State of North Carolina

Department of Health and Human Services

Division of Child and Family Well-Being



Crossroads MIS

Maintenance and Enhancement Services

North Carolina WIC Program

Appendix F

Disaster Recovery and Contingency Plan

Draft

Note: This draft Disaster Recovery and Contingency Plan is the approved plan from North Carolina's Child and Adult Care Food Program (CACFP) MIS system (NC Connects) which we host and support in the Azure cloud. Because cloud hosting is dramatically different from on-premises hosting and NC WIC is planning to move Crossroads to the cloud, Voyatek will be updating this plan for WIC during the project with the specific details applicable to the Crossroads WIC MIS.

Table of Contents

Acronyms	1
Document Identification.....	2
Revision History	2
1 Overview.....	3
2 GCOM Business Processes	3
2.1 GCOM Disaster Recovery Plan	3
2.2 Physical Environment	4
2.3 Team Environment	5
2.4 Disaster Declaration.....	5
2.5 GCOM Disaster Recovery Team	5
3 State Contacts	7
3.1 Notification.....	7
4 Mitigation Strategies	8
4.1 GCOM Staff Availability	8
4.2 System Data (Database)	8
4.2.1 High Availability.....	8
4.2.2 Cloud Backups.....	9
4.2.3 Offsite Backups.....	9
4.3 Files/Documents.....	9
4.4 Application Containers.....	10
5 Disaster Recovery Testing	10
6 Disaster History	10

Table of Figures

Figure 1: High Availability Architecture as Implemented in Azure	9

Table of Tables

Table 1: Definition of a Disaster.....	5
Table 2: GCOM's disaster recovery plan contacts	6
Table 3: State's disaster recovery plan contacts.....	7

Acronyms

Acronym	Description
CACFP	Child and Adult Care Food Program
DR	Disaster Recovery

Document Identification

Identification	Description
Document Name	NC CACFP Disaster Recovery Plan
Document Version	001
Document Status	<i>DRAFT</i>

Revision History

Name	Date	Description of Changes	Version
Jon Moreau	7/27/2023	Initial Document creation	1

1 Overview

This plan outlines the disaster and recovery procedures for the North Carolina Child and Adult Care Food program system in the event of a disaster that impacts GCOM facilities or operations. This plan addresses GCOM support during a disaster recovery event impacting North Carolina facilities or operations with respect to the CACFP system. This plan covers the procedures for declaring a disaster and communicating with state staff, interim business operations, and the steps to resume full operational capacity.

This plan will focus on the restoration of services including:

- System development
- Test environment availability
- Production system availability
- Help desk support
- Project management and coordination

2 GCOM Business Processes

2.1 GCOM Disaster Recovery Plan

A disaster is a sudden or non-predicted event that jeopardizes the ability of GCOM to deliver services to North Carolina. A disaster can include both natural and man-made events as defined later within this document. Short of a disaster is a disruptive event which is anything that puts operations at risk and can range from a cyberattack to a natural disaster. The GCOM disaster recovery (DR) and business continuity (BC) plans contain processes involved in the preparation for DR including planning and testing. In some cases, it can list a separate physical backup site for restoring operations.

GCOM takes steps to mitigate failure and risks by utilizing modern and secure techniques in architecture design and monitoring for and protecting infrastructure and data. Those techniques include encryption, vulnerability scanning, behavior analysis, network segmentation, frequent backups/snapshots, and geographic backup systems.

For the CACFP project, all essential tools will reside within Microsoft's Azure cloud. Source control, test scripts and issue management will reside in Azure DevOps Services (Microsoft's cloud-hosted version). Azure DevOps Service has cross-region redundancy and is designed to be highly available¹.

¹ Microsoft Online Service SLAs (including Azure DevOps Services and Office 365/SharePoint)

<https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services?lang=1>

This capability will allow GCOM team members to continue to access key project resources throughout almost any potential disaster event.

GCOM will also use the Microsoft Azure hosted SharePoint service to allow for high availability to project archives and documentation.

The GCOM DR plan is intended to address the availability of development, test, and production environments. These environments will be maintained and hosted by GCOM.

When required, GCOM staff conducts DR planning and collaborates with the project stakeholders accordingly to develop and implement a feasible plan considering different variables of the project and organization. The plan delineates the activities, resources, and responsibilities for all involved parties when a disaster occurs.

This plan will describe recovery mechanisms to allow for the restoration of core services in a short time period (1 hour) and organizational recovery mechanisms to return to full operational capacity within 72 hours.

Creating the DR plan ensures that the end users can focus on operations and not systems' availability and stability. The typical steps in our DR planning include:

1. Inventory of IT resources—Collecting data on all relevant IT resources (e.g., data hardware, software, etc.) supporting the project.
2. Inventory of operations—Gathering the input from key stakeholders to identify operations that are potentially at higher risk, incident scenarios, and responsible parties for resolving the issues.
3. Recovery timeline—Working with stakeholder(s) to set recovery goals and timeframes by which certain systems need to be back in operation including Recovery Point Objective (i.e., time since last backup) and Recovery Time Objective (i.e., time to recovery).
4. Data backups—Safeguarding a recent copy of all data assets for mission-critical applications.
5. Human risk—Mitigating the possibility of humans being a source of disaster, intentional or not.
6. DR plan testing—Ensuring the plan is drafted, bench tested, and complete so it is actionable and effective in case of a disaster.
7. Business Continuity (BC)—BC is the organization-wide strategy to maintain essential operations during and after a disaster. The BC plan should incorporate the DR plan to ensure complete preparation to meet any unexpected circumstances.

2.2 Physical Environment

GCOM will not be hosting any instances of the system (test or production) at company-owned facilities. All hosting will be in the Microsoft Azure cloud. Physical environment security is the responsibility of the cloud hosting provider .

2.3 Team Environment

The team operates from facilities located in Overland Park, KS, Columbia, MD, and Richmond, VA. Additional team members work from geographically dispersed locations within the United States.

2.4 Disaster Declaration

Definition of a Disaster: A disaster is a sudden or non-predicted event that jeopardizes the ability of GCOM to deliver services to the state as defined within the contract. A disaster can include both natural and man-made events, as categorized in Table 2 below:

Table 1: Definition of a Disaster

Natural	Man-Made
Earthquake	Arson
Flooding	Bomb damage/hoax
Hail	Break-in
Hurricane	Riot
Ice Storm	Strike
Lightning	Terrorism / Cyber Attack
Snowstorm	Vandalism
Sunspots	Explosion
Thunderstorm	Fire
Tornado	Water leak
Tsunami	Telecommunications Failure

A disaster will be declared if the production environment is non-operational or expected to be non-operational for 24-hours. This duration does not imply that no action will be taken for shorter outages. Members of the GCOM management team will initiate the disaster management protocol in the event of a qualifying disaster.

Once a disaster has been declared, GCOM staff will utilize this plan to initiate communications with state staff, coordinate with GCOM staff, and to execute plans to restore hosting services. Systems used to support the project will be brought back up (possibly in a different hosting region) within 72 hours. Once the disaster has been resolved, GCOM will coordinate with state staff to schedule the return of services to the primary hosting region with a minimum of project disruption.

2.5 GCOM Disaster Recovery Team

The following key staff included in Table 3 below will be responsible for leading the GCOM response to disaster recovery events.

Table 2: GCOM's disaster recovery plan contacts

Staff Name	Role	Phone	E-Mail
Monique Andrean	Project Manager	646-235-8829	monique.andrean@gcomsoft.com
Jim Ewald	VP Managed Services	919-448-8607	jim.ewald@gcomsoft.com
Krushanu Majmundar	Systems Recovery Coordinator	443-681-7474	Krushanu.Majmundar@gcomsoft.com
Jon Moreau	Technical Architect	913-908-7899	jon.moreau@gcomsoft.com
Ashwini Kamath	Database Administrator	801-989-0503	ashwini.kamath@gcomsoft.com
Jay Saunders	Nutrition Practice Director	913-707-0389	Jay.Saunders@gcomsoft.com

3 State Contacts

In the event of a disaster or a smaller service disruption, GCOM will utilize the below TBD contact list to communicate with state staff and to coordinate services during the disaster event.

The following individuals will serve as the contacts for the state:

Table 3: State's disaster recovery plan contacts

Staff Name	Role	Phone	E-Mail

3.1 Notification

Short Term Event: The most common short-term events are the loss of power or telecommunications for one or more team members. In the event of a short-term event, it will be the responsibility of the GCOM project manager to notify either the CACFP product director or an identified distribution list from the state of the nature of the disruption and the affected team members. The goal will be to provide alternate contacts or workaround communication methods for the impacted individuals. This communication will be provided as soon as possible and will be within 60 minutes of the identification of the event.

Disaster Event: If GCOM has determined that a disaster will impact routine operations for more than 24 hours, the decision to execute the disaster recovery plan to relocate operations to a secondary facility will be made. Once this determination has been made, the GCOM product manager or a company executive will contact state staff within one hour to notify them of the initiation of the disaster recovery plan. This communication will include:

- Guidance on effective/available communication methods during the disaster event.
- Assignment of non-affected staff providing support during the disaster event.
- Establishing the communication mechanism for regular status updates regarding the disaster.

Regular updates regarding the status of disaster recovery execution will be provided during the transition period. Following the disaster event, the GCOM product manager will coordinate the orderly return to normal business operations in a manner that minimizes disruption to the team's operations.

4 Mitigation Strategies

4.1 GCOM Staff Availability

The primary objective in response to either short- or long-term disruptions to operations will be the ability to provide the state with help desk and technical support as required within the contract. The proposed GCOM team include project management, business analysis, quality assurance, and technical resources that reside in geographically disparate locations. This aspect of the proposed team will allow GCOM to continue to provide each of those service elements even in the event of a regional disruption without investing in redundant staffing capacity.

The primary determination needed in the event of a disaster will be assessing telecommunication capabilities and responding to any outages. If GCOM determines that phone routing equipment is operational, help desk lines will be rerouted to available staff. In the event the phone lines are down, the GCOM product manager will contact state staff to provide secondary phone numbers for support services. These will be cellular numbers for remote staff that will be documented in the project staff contact documentation. The use of teleconference tools should not be affected and will continue to be available.

Most GCOM staff members are equipped with laptop computers. In the event of a facility disruption, they can continue to provide services from home or other office locations. Every attempt will be made to continue operations using laptop equipment, cellular communications, and organizational procedures in the event of a disaster.

4.2 System Data (Database)

4.2.1 High Availability

The system uses the Postgres Flexible Server offering from Azure to store transactional data, in both development/test and production environments. This is a fully managed database service which is configured for high availability with zone redundancy² in production (development/test is not configured for high availability). Azure's uptime SLA for Flexible Server with high availability enabled is 99.99%.

The following diagram shows the high availability architecture as implemented in Azure.

In addition to the highly available environment, backups of the database (that are managed in Azure) are stored in a geographically redundant location. The entire server can be restored from these backups to a secondary paired region³.

² For more information on the high availability architecture, see: <https://learn.microsoft.com/en-us/azure/postgresql/flexible-server/overview#architecture-and-high-availability>

³ For more information on geo-redundant backups, see <https://learn.microsoft.com/en-us/azure/postgresql/flexible-server/concepts-backup-restore#geo-redundant-backup-and-restore>

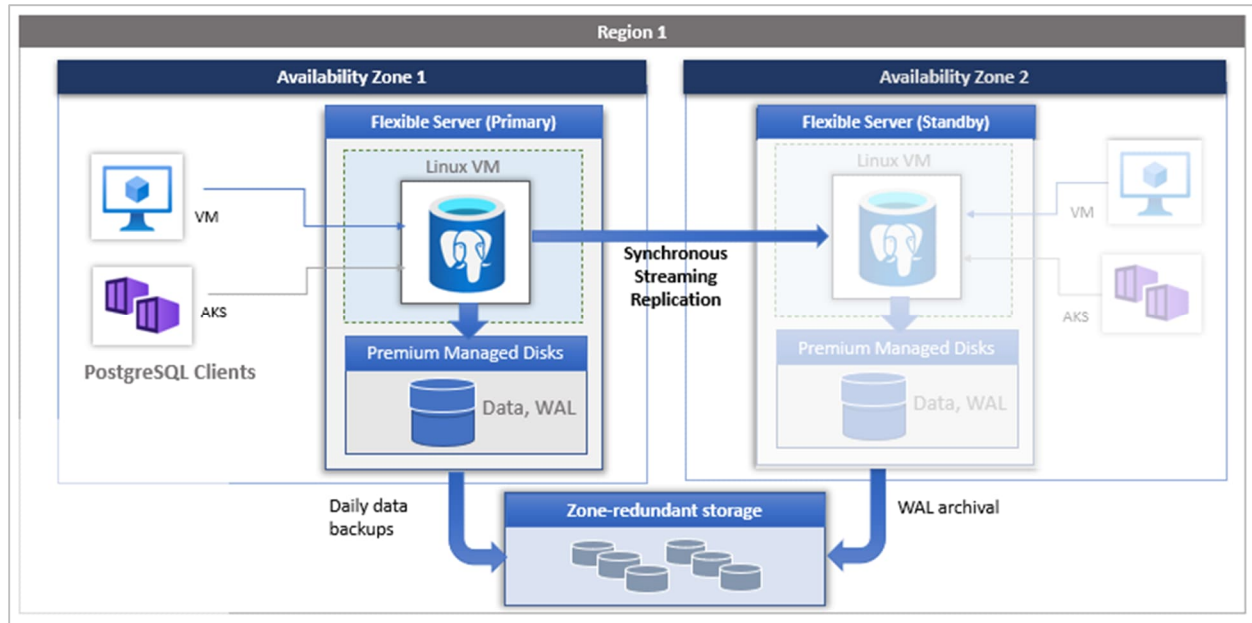


Figure 1: High Availability Architecture as Implemented in Azure

4.2.2 Cloud Backups

Flexible Server takes snapshot backups of data files and stores them securely in zone-redundant storage. The server also backs up transaction logs, which can be used to restore it to any point in time within the configured backup retention period⁴. The retention period is set to 35 days for production and 7 days for development/test. All backups are encrypted through AES 256-bit encryption for data stored at rest.

4.2.3 Offsite Backups

GCOM will provide access to an Azure storage location to allow North Carolina to take possession of backups on any schedule desired.

4.3 Files/Documents

Files (user-uploaded documents, system documents, and generated files, such as for payments) are stored in an Azure storage account. In production, this account is configured with geo-zone-redundant storage, which means storage is redundant across three availability zones in the deployed region (East US) as well as to a secondary region (West US), where it is also stored across three availability zones. GZRS is designed to provide at least 99.99999999999999% (16 9's) durability of

⁴ For more information on the general backup strategies used by Flexible Server, see <https://learn.microsoft.com/en-us/azure/postgresql/flexible-server/concepts-backup-restore>

objects over a given year⁵. For development/test, storage is configured with local redundancy, which provides at least 99.999999999% (11 nines) durability of objects over a given year.

4.4 Application Containers

The application code runs on containers hosted in Azure App Services. The service is configured to be highly available, with running containers distributed across all availability zones in the deployed region. There are three zones in the region, so there are always at least 3 containers of each system component running (API and identity service). Azure will deploy additional container instances as needed to support system demand, and any additional containers are also spread over all availability zones.

5 Disaster Recovery Testing

GCOM primarily performs disaster recovery tests in compliance with contracts that include disaster recovery testing provisions. These are typically performed on a yearly basis. Due to the nature of high availability for the production environment with data center redundancy in every tier disaster recovery is managed by Azure.

6 Disaster History

GCOM has not experienced any disasters in the last three years.

⁵ For more information on storage redundancy in Azure, see: <https://learn.microsoft.com/en-us/azure/storage/common/storage-redundancy>

Appendix G: Security and Vulnerability Plan

The following pages provide NC WIC the Security and Vulnerability Plan which describes Voyatek's audited security and vulnerability management processes based on SOC 2 Trust Services principles. The North Carolina Crossroads Maintenance and Enhancement project will fall under Voyatek's security umbrella and be included in yearly SOC 2 audits following contract execution.

State of North Carolina

Department of Health and Human Services

Division of Child and Family Well-Being



Crossroads MIS

Maintenance and Enhancement Services

North Carolina WIC Program

Appendix G

Security and Vulnerability Plan

Draft

Note: This draft Security and Vulnerability Plan is the approved plan from North Carolina's Child and Adult Care Food Program (CACFP) MIS system (NC Connects) which we host and support in the Azure cloud. Because cloud hosting is dramatically different from on-premises hosting and NC WIC is planning to move Crossroads to the cloud, Voyatek will be updating this plan for WIC during the project with the specific details applicable to the Crossroads WIC MIS.



Contents

Document Identification	1
Edit History	1
Document Approval	1
1. Introduction	2
2. Overview.....	2
2.1 System Overview.....	2
2.2 System Architecture	2
2.3 Physical and Environmental Security.....	2
2.4 Data Classification.....	2
2.5 Data Storage	2
2.6 Data Transmission.....	2
2.7 Data Sharing	3
2.8 Network Segmentation	3
2.9 Network Security Controls	3
2.10 Containers and Orchestration.....	3
2.11 Identity Management.....	3
2.12 Application Security Controls	3
2.13 Remote Access	4
2.14 Development Practices	4
2.15 Deployment Processes.....	4
2.16 Instrumentation, Logging, and Telemetry.....	4
2.17 Vulnerability Assessments and Mitigation	4
3. System Overview	4
4. System Architecture	6
4.1 Conceptual Architecture	6
4.1.1 API	7
4.1.2 Client.....	7
4.1.3 Database and Cache	7
4.1.4 Identity Management	7
4.1.5 Logging and Metrics	7
4.1.6 Realtime Communications	8
4.1.7 Workers.....	8
4.2 Physical System Architecture	9
4.2.1 Virtual Private Networks.....	9
4.2.2 Container Orchestration	9

4.2.3	Public Access, DNS, and Load Balancing	10
4.3	Physical and Environmental Security	10
4.3.1	Hosting Environment	10
4.3.2	Voyatek and Third-Party Facilities	11
4.4	Data Classification	11
4.5	Data Storage	11
4.5.1	Container Orchestrator	12
4.5.2	Blob Storage	12
4.5.3	Container Storage	12
4.5.4	Database	12
4.5.5	Cache	12
4.5.6	Logging and Telemetry	12
4.5.7	Virtual Machines	13
4.6	Data Transmission	13
4.6.1	Inside the Hosting Environment	13
4.6.2	External Access	13
4.7	Data Sharing	13
4.7.1	Data Conversion	13
4.7.2	Identity Provider	14
4.8	Network Segmentation	14
4.8.1	Virtual Networks	15
4.8.2	Subnets	15
4.9	Network Security Controls	16
4.9.1	Virtual Networks	16
4.9.2	Subnets and Network Security Groups	16
4.9.3	Port Rules	17
4.10	Containers and Orchestration	17
4.10.1	Overview	17
4.10.2	Containers	17
4.10.3	Repositories	18
4.10.4	Orchestration	18
4.11	Identity Management	20
4.11.1	Hosting Environment	20
4.11.2	System	20
4.11.3	Auditing	21
4.11.4	Profiles	22
4.12	Application Security Controls	22

4.13	Remote Access	24
4.13.1	Jump Box.....	24
4.13.2	AKS Control Plane	24
4.14	Development Practices	25
4.14.1	Access Controls	25
4.14.2	Code Review.....	25
4.14.3	Automated Build Processes	25
4.15	Deployment Processes.....	25
4.15.1	Environment Preparation.....	25
4.15.2	Scope of Responsibilities.....	27
4.16	Instrumentation, Logging, and Telemetry.....	28
4.16.1	Instrumentation	28
4.16.2	Logging.....	29
4.16.3	Telemetry	30
4.17	Vulnerability Assessments and Mitigation	31

Figures

Figure 1: CACFP System Overview	5
Figure 2: Conceptual System View	6
Figure 3: Physical System Architecture.....	9
Figure 4: FTP Process Workflow	14
Figure 5: Interaction Flow	21
Figure 6: Permission Sets Schema	23
Figure 7: Terraform Tool Sample Illustration	27
Figure 8: sample CPU metrics.....	28
Figure 9: Structured Logging Example	29
Figure 10: Application Insights Query Example	30

Tables

Table 1: Document Identification	1
Table 2: Document Edit History.....	1
Table 3: Document Approvals	1

Document Identification

Table 1: Document Identification

Identification	Description
Document Name	Security & Vulnerability Plan
Project Name:	CACFP
Project Sponsor(s) Name	Rahul Puri
Project Manager	Monique Andrean
Document Version	DRAFT
Document Status	DRAFT
Data Submitted	June 13, 2022
SharePoint Location	Security and Vulnerability Plan-DRAFT

Edit History

Table 2: Document Edit History

Version	Date	Section Changed/Description	Prepared by
DRAFT	06/09/2022	Document Creation	Jon Moreau
DRAFT 2	07/22/2022	Addressed comments from NC CACFP (Jason Gilmore)	Jon Moreau/ Jay Saunders

Document Approval

Table 3: Document Approvals

GCOM		
Name	Role	Date
Patrick Connor	VP of Security and Infrastructure	
Jay Saunders	Sr. Director, Product Management	
Monique Andrean	Project Manager	
NC-CACFP		
Kim Lovenduski	Project Director- Deputy Director, Community Nutrition Services Section	
Cassandra Williams	Business Owner/Lead, CACFP	
Sharon McDougal	IT Services Manager, DCFW, Community Nutrition Services Section	
Tarun Karani	Project Manager	

1. Introduction

This document outlines Voyatek's approach for securely building, deploying, and maintaining the CACFP application.

2. Overview

This document has been divided into several sections, each of which are briefly described here.

2.1 System Overview

This section provides a brief overview of the CACFP MIS, including functionality, users, and data.

2.2 System Architecture

This section describes the system's planned architecture, from both application design and deployment perspectives.

2.3 Physical and Environmental Security

This section describes the physical and environmental protections made available by the hosting provider, Microsoft Azure, as well as the protections employed by Voyatek at its facilities.

Requirements/Guidelines Source(s)

- [North Carolina SCIO-SEC-313 Physical and Environmental Protection Policy](#)

2.4 Data Classification

This section outlines the types of data stored in the system and assigns classification levels to each of them. It also describes how data classification affects system design.

Requirements/Guidelines Source(s)

- [North Carolina Statewide Data Classification & Handling Policy](#)

2.5 Data Storage

This section describes how system data will be kept secure while at rest (that is, retained on storage media in the hosting environment).

Requirements/Guidelines Source(s)

- [North Carolina Statewide Data Classification & Handling Policy](#)
- [North Carolina SCIO-SEC-316 System and Communications Protection Policy](#)

2.6 Data Transmission

Data is continuously being transmitted between system components (in the hosting environment) and between end users of the application and the hosting environment. Keeping these communications private and safe from tampering is important so that system data remains confidential. This section describes the measures employed by the system to keep communications secure.

Requirements/Guidelines Source(s)

- [North Carolina SCIO-SEC-316 System and Communications Protection Policy](#)

2.7 Data Sharing

This section describes the types of data that are shared outside the system and with what external systems data is shared. It also describes formal agreements that are in place to govern data exchange with external systems.

2.8 Network Segmentation

The components that comprise the deployed system are deployed to different logical network segments. For example, client-facing components (such as the web client or the system's API) reside in network segments that allow users to connect to them directly. Database instances, on the other hand, only accept connections from specific endpoints in the system, such as from API components. This section describes the network segmentation strategy for the system and outlines which components are deployed to each network segment.

Requirements/Guidelines Source(s)

- [North Carolina SCIO-SEC-316 System and Communications Protection Policy](#)

2.9 Network Security Controls

Network security controls prevent unauthorized traffic from reaching application components. This section describes how network security controls are defined in the system and how they are implemented in the hosting environment.

Requirements/Guidelines Source(s)

- [North Carolina SCIO-SEC-316 System and Communications Protection Policy](#)

2.10 Containers and Orchestration

The system is built from deployable containers which are run on a container orchestration framework in the hosting environment. This section will outline how containers and the orchestration environment are secured.

Requirements/Guidelines Source(s)

- [North Carolina SCIO-SEC-317 System and Information Integrity Policy](#)
- [North Carolina SCIO-SEC 318 Supply Chain Risk Management](#)

2.11 Identity Management

Managing user identities is a foundation on which many other security controls rest. This section will discuss how user identities are managed in the hosting environment and in the system.

Requirements/Guidelines Sources

- [North Carolina SCIO-SEC-301 Access Control Policy](#)
- [North Carolina SCIO-SEC-307 Identification and Authentication Policy](#)

2.12 Application Security Controls

The system manages user access rules using assigned roles and permissions. This section outlines how the system applies access restrictions to users on a per-request basis.

- [North Carolina SCIO-SEC-301 Access Control Policy](#)
- [North Carolina SCIO-SEC-307 Identification and Authentication Policy](#)

2.13 Remote Access

Remote access to the system components in the hosting environment is tightly controlled. This section will cover how remote access is provisioned and what components are accessible remotely.

Requirements/Guidelines Source(s)

- [North Carolina SCIO-SEC-301 Access Control Policy](#)
- [North Carolina SCIO-SEC-307 Identification and Authentication Policy](#)

2.14 Development Practices

The system is only as safe as the development practices that go into making it. This section describes the steps we take to make sure that code management and build processes are secure.

Requirements/Guidelines Source(s)

- [North Carolina SCIO-SEC 318 Supply Chain Risk Management](#)

2.15 Deployment Processes

The system is designed to be deployed in an automated fashion. This section will discuss the tools and processes we use to automate deployments, and how they enhance system security.

Requirements/Guidelines Source(s)

- [North Carolina SCIO-SEC 318 Supply Chain Risk Management](#)

2.16 Instrumentation, Logging, and Telemetry

The system exposes a rich set of instrumentation, logging, and telemetry data. This section outlines how that data is generated, stored, and made available, with a view to how this enhances system security.

Requirements/Guidelines Source(s)

- [North Carolina SCIO-SEC-317 System and Information Integrity Policy](#)

2.17 Vulnerability Assessments and Mitigation

The system will be evaluated periodically to ensure that no common application vulnerabilities are found. In addition, penetration testing will be conducted on the overall system. This section outlines the tools and practices Voyatek will use to conduct these evaluations.

Requirements/Guidelines Source(s)

- [North Carolina SCIO-SEC-317 System and Information Integrity Policy](#)

3. System Overview

The system provides program management functions for the CACFP program, which is one of several programs under the Child Nutrition Program umbrella. The system is used primarily by state employees who administer the program and by participating institutions who provide program benefits to participants and who are reimbursed by the program for that work. In addition, state and

federal program auditors will access the system to verify that the program is being administered in compliance with federal and state regulations.

The system consists of several key components:

- General program management
- Managing applications, both initial and renewal
- Managing claims submitted to the program and the payment of those claims
- Managing compliance to program rules and regulations by participating institutions
- Providing reports and other analytics to stakeholders

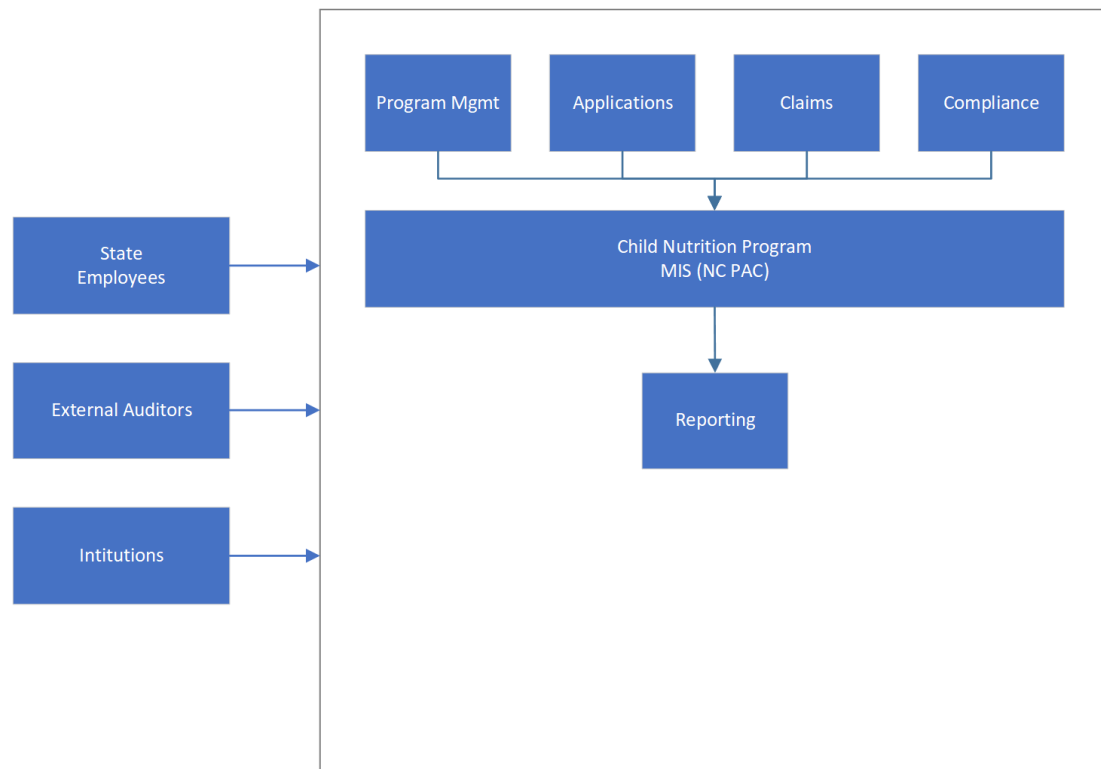


Figure 1: CACFP System Overview

4. System Architecture

The CACFP MIS is an API-centric system that includes a client application for end users, an identity management subsystem that handles federated authentication, a real-time communications bus, and supporting “worker” components that handle batch processing and external communications.

4.1 Conceptual Architecture

The following diagram shows a conceptual view of the system.

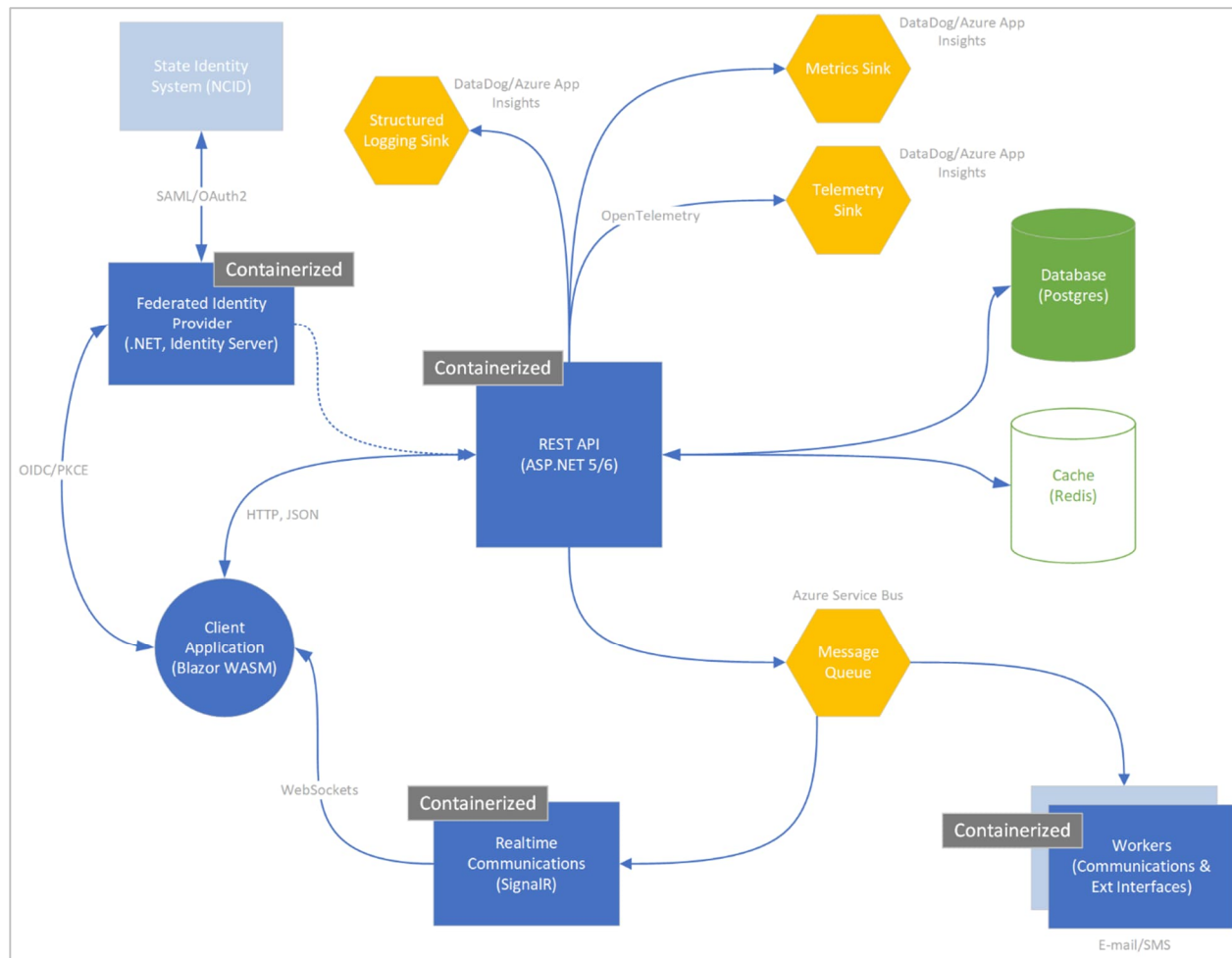


Figure 2: Conceptual System View

4.1.1 API

The API will be built in the REST (Representational State Transfer) style, using the Microsoft .NET platform, and will be deployed using Linux containers to the cloud hosting environment. Because they contain both the application and its dependencies in one place, containers make deployment much more straightforward. In addition, container resources can easily be scaled up and down to meet current demand.

Virtually all the business logic in the system will be in the API. This means that the system's other components (such as the client) can be updated or changed as needed without impacting the core functionality of the system. This will extend the useful life of the system.

4.1.2 Client

The client software is intended to provide a rich experience for users no matter how they access the system. Primarily, it will be designed for desktop users, but users on mobile devices will have a good experience as well. Microsoft's Blazor technology has been chosen because of its tight integration with the rest of the technology stack and its excellent performance.

4.1.3 Database and Cache

The system will utilize PostgreSQL as the transactional database, with Redis serving as a distributed cache. PostgreSQL is widely used by both large and small organizations, and it has a feature set that is very similar to both SQL Server and Oracle RDBMSs. It offers substantial cost savings because it is open-source and typically runs on Linux. This avoids licensing fees for both the Windows operating system and for the RDBMS itself.

4.1.4 Identity Management

The system will leverage NCID as a federated identity provider using NCID's SAML capabilities. This means that the system will not maintain user credentials, but instead will rely on NCID to authenticate users. An intermediate authentication component based on the open-source Identity Server product will be part of the system, and it will serve to insulate the MIS from the specifics of integrating with NCID. OpenID Connect is the basis for the application's authentication features, and PKCE (Proof Key for Code Exchange) will be used to prevent forgery attacks when users sign into the client.

4.1.5 Logging and Metrics

The system has logging, metrics, and telemetry subsystems. The data captured by these will be stored in Azure's Application Insights service for easy querying and analysis.

- Logging uses structured log events where the data in the log message is also available as individual data elements. For example, a log that says, "User with ID '123' logged in" would be stored not only as text, but it would also have a UserId field in the log with the value "123." This enables much more precise use of the log as a troubleshooting and diagnostics tool.
- The system offers metrics data collection endpoints for all running containers. This allows system administrators to easily understand system performance, identify system components that are having problems, and it also allows the container management infrastructure to scale the system up and down based on load.
- Telemetry is captured in every system component from the API down. This allows data flow through the system to be captured and those traces viewed. The telemetry information

enables detailed monitoring of system performance down to the method call level, and it also provides a view across components.

More information on the instrumentation, logging, and telemetry data produced by the system can be found in the section of the same name at the end of this document.

4.1.6 Realtime Communications

The system includes a real-time communication bus that links the API and client applications together. This will enable rich communications scenarios in areas of the application where real-time collaboration is required.

4.1.7 Workers

The “workers” are long running processes, hosted in containers, which do things like run batch processing tasks or send e-mails/texts from an outbound message queue.

4.2 Physical System Architecture

The following diagram depicts the physical system architecture (as deployed to the Azure hosting environment). Note that this information may be subject to change as refinements are made.

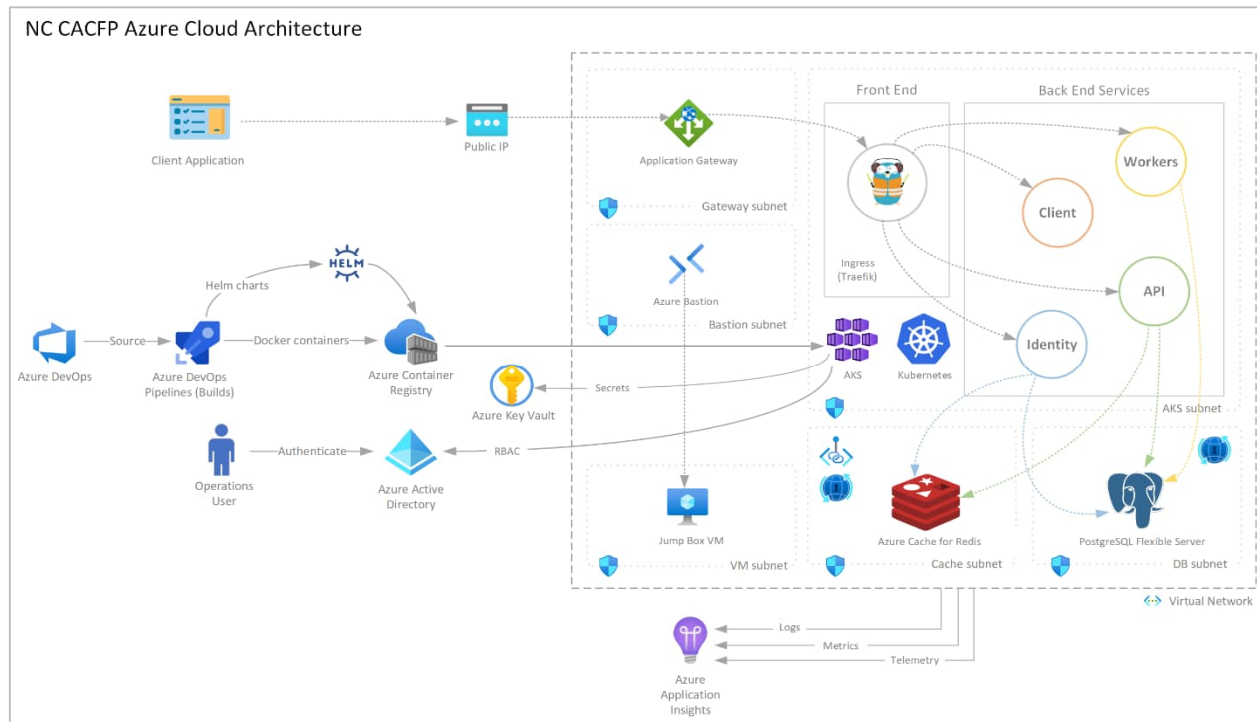


Figure 3: Physical System Architecture

As outlined earlier in this document, the CACFP system will be hosted in the Microsoft Azure cloud and will utilize several PaaS (Platform as a Service) offerings that are part of Azure, such as PostgreSQL, Redis (for caching), and Application Insights (for logging and telemetry). The nature of consuming cloud PaaS offerings in this way means that, as a vendor, we have delegated the responsibility for managing things like routers, firewalls, and switches to the cloud vendor. This lack of control over physical infrastructure is not a negative—the system can benefit from the cloud provider's expertise in managing network infrastructure and both vendor and customer can enjoy the benefits of simpler security configuration without having to manage network infrastructure.

However, there are several services/strategies that will be used when making the system publicly available for test and production environments that leverage cloud security features to keep the system secure.

4.2.1 Virtual Private Networks

Publicly accessible environments (test and production) will be isolated in a private network which is divided into subnets. This means that back-end services and applications will not be directly exposed to the Internet. The most critical components that will be isolated are those that store data (database and cache) and application components such as the API and identity provider.

4.2.2 Container Orchestration

The current plan for test and production environment deployments is to use a container orchestration service (such as Azure Kubernetes Service) to host the application. This adds another

layer of isolation to the app's deployment. The cluster (group of computing resources that provides the app's functionality) is linked to a virtual network or VNet. In addition, the cluster has clearly defined ingress and egress rules that are used to control traffic. Clusters can also enforce rules that govern communication between components in the cluster, such as requiring mutual TLS to secure communications between them.

4.2.3 Public Access, DNS, and Load Balancing

Deployments will likely follow the blue/green model, where a deployment consists of standing up a completely new environment and then redirecting traffic to the new environment. The old environment is then destroyed. This kind of deployment is extremely difficult in a traditional data center environment, but with automated deployments to a containerized infrastructure, it is much simpler. For it to work, a layer is needed over the app to route traffic from end users into the correct environment. This layer can also perform duties like traffic filtering, geographic access restrictions, and load balancing. We plan to utilize an ingress controller in Kubernetes called Traefik, along with edge services from Azure (such as Front Door and/or load balancing) to realize these goals.

4.3 Physical and Environmental Security

4.3.1 Hosting Environment

Keeping the data center environment where the system is deployed secure is critically important to the overall security of the system. Physical security vulnerabilities might allow an attacker to gain access to network traffic or to the physical storage media where system data is stored. Since the system is hosted in a Microsoft Azure data center, it benefits from the robust physical security infrastructure used at all Azure data centers.

Microsoft publishes regularly updated documentation outlining the security measures in place at their data centers¹. Some highlights:

- Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means.
- Authorized staff and visitors must pass two-factor authentication with biometric scanning to access data center floors. Only approved devices are allowed, and everyone must pass through a metal detector upon entry and exit from the data center floors.
- Microsoft uses a hard drive wiping solution that is NIST 800-88² compliant. Hard drives that cannot be wiped are disintegrated, shredded, pulverized, or incinerated, and records of the destruction are retained.

A full list of the Azure compliance offerings is published by Microsoft here:

<https://docs.microsoft.com/en-us/azure/compliance/>

¹ <https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security>

² <https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final>

4.3.2 Voyatek and Third-Party Facilities

Voyatek requires employees and contractors to record entry and exit (using badges) when working at company-owned facilities.

During development, some data for the system (particularly customer databases to be converted/migrated) is housed in a third-party data center managed by TierPoint. TierPoint provides data center services, which includes implementing physical security controls to protect the housed in-scope systems. Controls include, but are not limited to:

- Visitors are required to sign in
- Access cards and biometric scans are required to move through the facility via controlled access points, and all access is logged
- Video surveillance and monitoring is in place throughout the data center facility

Voyatek currently uses the TierPoint hosting facility located in Baltimore, Maryland, with a secondary facility in Raleigh, North Carolina. All data is maintained within US hosting facilities.

4.4 Data Classification

Voyatek has reviewed the North Carolina Data Classification and Handling Policy. Based on this review, Voyatek proposes that CACFP system data meets the Medium Risk data classification and proposes to utilize Restricted data handling procedures.

4.5 Data Storage

Several components of the system store data. All the components always encrypt data at rest. The system is comprised of both containers and Platform-as-a-Service (PaaS) offerings from Azure:

- **Container orchestrator:** Azure Kubernetes Service (AKS) manages storage for containers (the deployable units that comprise the system: client, API, identity management, real-time communications, and workers)
- **Blob storage:** Azure Storage stores document data
- **Container storage:** Azure Container Registry (ACR) stores the deployable containers
- **Database:** Azure Database for PostgreSQL is the database engine that the system uses to store application data
- **Cache:** Azure Cache for Redis holds frequently accessed data
- **Logging and telemetry:** Azure Application Insights stores logging and telemetry data
- **Remote access:** A virtual machine is used as a jump box to provide remote access to system components (custom and PaaS)

The sections below outline how each component stores data at rest securely. For more information on the technical aspects of these components, see the *System Architecture* section at the beginning of this document.

4.5.1 Container Orchestrator

By default, when using Azure Kubernetes Service (AKS), OS and data disks use server-side encryption with platform-managed keys. The caches for these disks are also encrypted at rest with platform-managed keys³.

4.5.2 Blob Storage

Data in Azure Storage is encrypted and decrypted transparently using 256-bit AES encryption and is FIPS 140-2 compliant. Encryption is enabled for all storage accounts and cannot be disabled. Data in a storage account is encrypted regardless of performance tier, access tier, or deployment model. All blobs in the archive tier are also encrypted. All Azure Storage redundancy options support encryption, and all data in both the primary and secondary regions is encrypted when geo-replication is enabled. All Azure Storage resources are encrypted, including blobs, disks, files, queues, and tables. All object metadata is also encrypted⁴.

4.5.3 Container Storage

Azure automatically encrypts content stored in Azure Container Registry (ACR) at rest with service-managed keys⁵.

4.5.4 Database

The Azure Database for PostgreSQL service uses the FIPS 140-2 validated cryptographic module for storage encryption of data at-rest. Data, including backups, are encrypted on disk, including the temporary files created while running queries. The service uses the AES 256-bit cipher included in Azure storage encryption, and the keys are system managed. Storage encryption is always on and cannot be disabled⁶.

4.5.5 Cache

The cache implementation used by the system does not persist any data (all data is stored in memory on the cache instance).

4.5.6 Logging and Telemetry

Because Application Insights uses Azure Storage to store persistent data, the data is encrypted at rest (see *Blob Storage*, above, for more detail).

³ <https://docs.microsoft.com/en-us/azure/aks/enable-host-encryption>

⁴ <https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption>

⁵ <https://docs.microsoft.com/en-us/azure/container-registry/container-registry-customer-managed-keys>

⁶ <https://docs.microsoft.com/en-us/azure/postgresql/single-server/concepts-security>

4.5.7 Virtual Machines

Disk encryption will be enabled for all disks attached to virtual machines (VMs).

4.6 Data Transmission

The bulk of the communication between the system and the outside world is with the client application, used by state staff and program participants. All communication between the client application and the central system components, hosted in Azure, is done over TLS⁷-secured communication links.

4.6.1 Inside the Hosting Environment

The main intent of isolating the system in a virtual network, or VNet (see the section **Network Segmentation**), is to prevent direct network access to any components in the system from the outside—either the Internet or other systems running in the cloud hosting environment. However, traffic between components should also be encrypted. Specifically, the following traffic will be encrypted using TLS or mTLS:

- All database connections use TLS 1.2 or newer
- All cache connection use TLS 1.2 or newer
- Inter-cluster traffic in AKS between the ingress controller and the containers, as well as inter-container calls

4.6.2 External Access

As mentioned, all inbound communication is secured with TLS 1.2 or greater. Specifically, this includes:

- Connections from the client application to the system
- Connections to the API from remote systems
- Remote access connections

4.7 Data Sharing

4.7.1 Data Conversion

During the data conversion effort, data will be transferred from North Carolina to Voyatek using FTPS (Secure FTP). Data to be converted will be uploaded to a state controlled FTPS site by state staff. Voyatek staff will download the data to a SQL Server database server located in the Voyatek data center. Initial conversion will migrate the SQL Server database to a PostgreSQL database for further work. After conversion is complete, a backup of the converted database will be uploaded to Azure Storage and restored from there to the cloud-based PostgreSQL database server. Once data migration is complete, all source data will be disposed of per secure data disposal standards.

⁷ TLS is a current standard for providing secure communications over public networks. Although the terms are often used interchangeably, TLS is a replacement for SSL. This document will use the term TLS to refer to this type of communications security.

4.7.2 Identity Provider

User authentication data will be transmitted from the North Carolina NCID system as part of the Single Sign-On (SSO) process for end users. Data will be transmitted over secured encrypted channels. Authentication data received from NICD will be cryptographically signed to ensure it has not been tampered with in transit.

4.7.2.1 Outgoing Communications

The system will allow state users to send emails to individuals and groups of program participants. These e-mails will contain notifications of system activity and events. They will not contain PII or financial information.

4.7.2.2 Financial Data

The system will periodically generate payment files and publish them to a state-controlled FTP server for pickup by downstream financial systems. The following diagram shows this workflow:

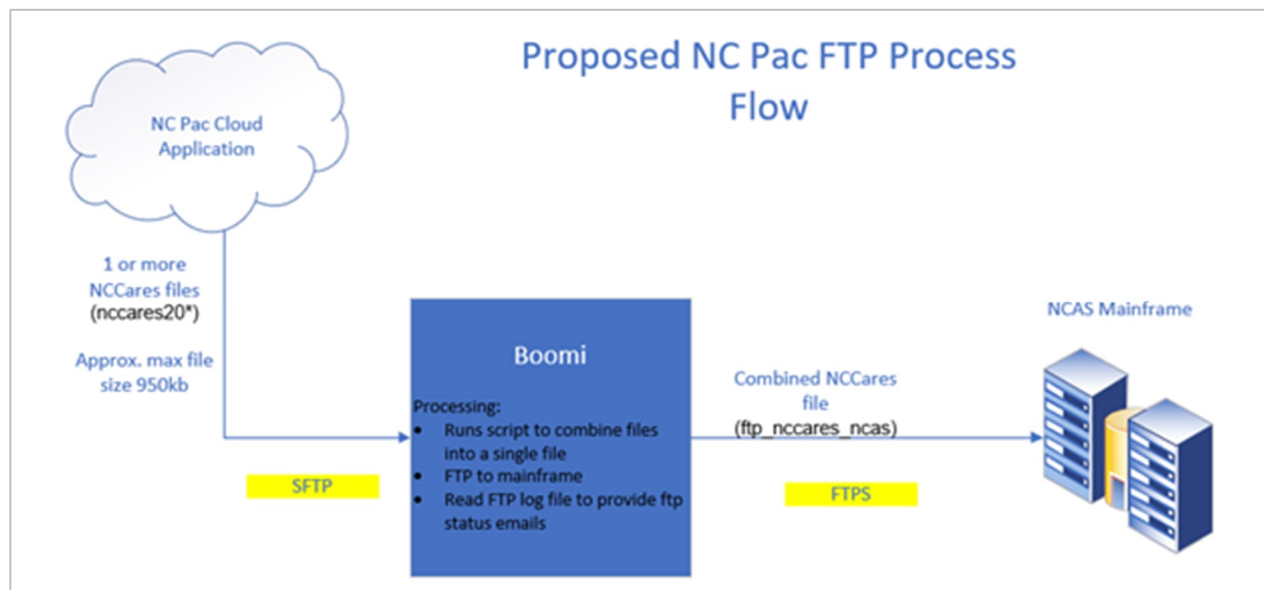


Figure 4: FTP Process Workflow

4.7.2.3 Claim Detail Data

Institutions will have the ability to import claims data in an industry-standard format into the system, via the client application.

4.8 Network Segmentation

In a traditional data center, the data network is divided into layers with increasingly strict access controls, typically enforced by layer 3 and 4 network devices and host-based firewalls, as you move deeper into the data center (from an external viewpoint).

In a cloud deployment, there is no control over (or even visibility to) the underlying network layer of the environment. However, there are several features in Azure that allow systems to be isolated from the rest of the environment.

4.8.1 Virtual Networks

Virtual networks isolate private network traffic from the shared cloud network infrastructure. Each deployed environment exists in an isolated virtual network. This allows complete control over ingress and egress traffic and a more flexible network segmentation strategy⁸.

There are some scenarios where data may be shared between environments. For example, it is common to periodically refresh the customer test environment with redacted production data. This can be accomplished by creating a peering connection between the two virtual networks and transferring the data. This keeps the data entirely in private networks. The peering connection can be removed when no longer needed.

4.8.2 Subnets

Architectural layers of the application are divided into subnets, each with their own access rules. Each virtual network contains six subnets:

- Orchestration subsystem (Kubernetes/AKS)
- Database (PostgreSQL)
- Cache (Redis)
- Application gateway (for application traffic)
- Virtual machines (for jump box/remote access)
- Bastion (for accessing the jump box remotely)

Subnets are shown on the physical architecture diagram that appears earlier in this document.

4.8.2.1 Orchestration Subsystem

This subnet contains only the Azure Kubernetes Service (AKS) instance⁹. This keeps the AKS instance separate from all other components with only configured network security rules permitting inbound traffic. AKS manages IP address assignment within the allocated space for the subnet, which is a /22 size (in CIDR notation).

4.8.2.2 Database

The PostgreSQL flexible server instance is associated with a subnet—in fact, the subnet cannot be used for any other items once configured this way. This allows Azure to allocate IP address assignments to the database system instances from the subnet without worrying about collisions. Networking is configured as “private access with VNet integration”¹⁰. This exposes the database endpoint at an IP inside the subnet range to the virtual network (so it can be accessed from other locations inside the private network, such as by components running in AKS).

⁸ For more information on Azure virtual networks and subnets, see: <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview>

⁹ For more information on AKS subnet integration, see: <https://docs.microsoft.com/en-us/azure/aks/configure-kubenet>

¹⁰ PostgreSQL network integration options are explained in more detail here: <https://docs.microsoft.com/en-us/azure/postgresql/flexible-server/concepts-networking>

4.8.2.3 Cache

Like the database server configuration, the Redis cache is configured in a subnet, with a private endpoint that allows access from other locations inside the virtual network¹¹.

4.8.2.4 Application Gateway

The application gateway subnet contains the gateway, linked to an external IP address so that it is reachable over the Internet (some environments may have additional ingress restrictions as well). The gateway forwards traffic to the AKS ingress controller, which then forwards it to the components that handle that traffic.

4.8.2.5 Virtual Machines

The use of virtual machines in this environment is limited to a single jump box that is used to allow operations personnel to remotely access system components to troubleshoot problems. The jump box is assigned to a subnet with assigned security rules. The jump box is only reachable from outside via Azure Bastion and cannot be connected to remotely any other way. See the next subheading for more information on Bastion.

4.8.2.6 Bastion

Bastion is an Azure product that allows for secure access to virtual machines. For this system, since the jump box exists in a private VNet, it can only be reached via Bastion. More detail on how the Bastion service works can be found in the **Remote Access** section of this document.

4.9 Network Security Controls

The hosting environment includes network-based security controls. There are three key components that provide this functionality at a low level:

- Virtual networks, or VNets, which serve as a container where all system traffic can be isolated (away from the hosting environment's main networking infrastructure)
- Subnets, or logical divisions of the VNet into smaller sections
- Network security groups, which apply ingress & egress rules to subnets
- Port rules at the container level

4.9.1 Virtual Networks

As discussed earlier in **Network Segmentation**, a VNet exists to isolate all the traffic for the system. It is associated with a class A private address block. This prevents all traffic from the hosting environment and from the Internet from reaching any component inside the VNet unless ingress is explicitly allowed. This forms the basis for further network security rules to be applied.

4.9.2 Subnets and Network Security Groups

Subnets are smaller logical groupings of address assignments. They are associated with network security groups that control ingress and egress for all components in the subnet. This allows the network to maintain a "flat" structure (within the single VNet) while providing for control over traffic

¹¹ Redis private VNet integration is documented here: <https://docs.microsoft.com/en-us/azure/azure-cache-for-redis/cache-private-link>

between components. There are security groups for all subnets, each with their own rules for what types of traffic is allowed.

4.9.3 Port Rules

Each container in the system (controlled by AKS) has certain defined ports that can be reached. The AKS service only accepts traffic on these ports when evaluating whether to pass ingress traffic on. Other types of access to the containers (such as SSH) must go through the AKS control plane.

4.10 Containers and Orchestration

4.10.1 Overview

The system's primary functionality is delivered in containers, which are a packaged unit of the custom code that makes up a system component together with its dependencies¹². Because containers hold both application code and dependencies together, they can be deployed as a unit. Typically, containers are managed by an orchestrator, which runs one or more sets of the containers required for the system to operate. The orchestrator monitors the health of the containers and can scale the number of container instances to match current system load, among other responsibilities.

4.10.2 Containers

Containers are created from “layers,” which are sets of either operating system (OS) data or other dependencies. A typical set of layers might include an OS base layer, required OS extensions or modules, and then platform specific dependencies, such as the Java Runtime Environment (JRE) or the .NET Runtime/SDK¹³.

The container is built up from the layers that comprise it, with the addition of compiled custom code, to create a complete, deployable unit. Base images (layers) are typically provided by trusted parties, but care must be taken to avoid supply chain attacks enabled by using images from untrusted sources. The system only uses three images for deployable components. The .NET-related base layers are provided and vetted by Microsoft¹⁴. The Nginx image (used to serve downloadable client application binaries) is provided by Docker¹⁵.

- mcr.microsoft.com/dotnet/sdk:6.0-alpine (this image is used to build the software from source)
- mcr.microsoft.com/dotnet/runtime-deps:6.0-alpine (this image is used for running compiled applications, such as the API and identity service)
- nginx:alpine

¹² For an introduction to containers and Docker, see: <https://docs.microsoft.com/en-us/dotnet/architecture/microservices/container-docker-introduction/>

¹³ For more detail on how containers are created from layers, see: <https://medium.com/geekculture/introduction-to-containers-basics-of-containerization-bb60503df931>

¹⁴ The Docker Hub repository page provides more information on these base images: https://hub.docker.com/_/microsoft-dotnet-sdk/

¹⁵ Nginx is an “official image” provided by Docker. For more information, see: https://hub.docker.com/_/nginx

All these images are built on Alpine Linux, a lightweight distro that includes only a minimum set of functionality. This streamlines deployment by keeping the container small, and it also avoids many potential vulnerabilities because it simply does not include any unneeded libraries/dependencies.

Vulnerability checks on containers are run using Docker's built-in vulnerability scanning tool. An example of a successful check (no vulnerabilities) for the client application container is shown below:

Package manager: apk

Project name: docker-image|cnpmis-client

Docker image: cnpmis-client:0.0.1

Platform: linux/amd64

Base image: nginx:1.22.0-alpine

✓ Tested 43 dependencies for known vulnerabilities, no vulnerable paths found.

This testing is conducted regularly as base images are updated and made available for use.

4.10.3 Repositories

Finalized images are versioned and then uploaded to a container registry. This system uses a container registry per environment, which is a best practice to keep environments isolated. Azure Container Registry (ACR) is used for the registry implementation. During deployments, the container orchestrator will pull images from the registry directly in order to create instances of each of the system's primary components.

Registries are integrated into Azure Active Directory (AAD) so that both publishing and pulling images requires a secure connection using a principal identity registered with AAD.

4.10.4 Orchestration

There are many technologies available for providing container orchestration. The most popular is Kubernetes, often abbreviated as K8s¹⁶. Kubernetes is an open-source platform for managing containerized workloads. This system uses a managed service for Kubernetes provided by Microsoft, called Azure Kubernetes Service (AKS)¹⁷. AKS allows Kubernetes implementations to be tied more closely into the Azure ecosystem.

From a security perspective, Kubernetes does introduce complexity to the operating environment. However, using a managed service like AKS reduces this complexity significantly. One key area that needs to be secured is the control plane API. GCOM uses IP-based security rules to ensure that only operations users at authorized facilities have permission to the connect to the control plane. In addition, access to the control plane API is restricted using role-based access (RBAC) tied into AAD. This means that corporate policies for managing user access are also applied to AKS instances. For example, if an employee leaves GCOM, their AAD account is suspended, which will immediately prevent them from accessing any AKS instances linked to AAD.

¹⁶ An overview of Kubernetes can be found here: <https://kubernetes.io/docs/concepts/overview/>

¹⁷ Microsoft AKS documentation can be found here: <https://docs.microsoft.com/en-us/azure/aks/>

4.11 Identity Management

4.11.1 Hosting Environment

Access to the cloud hosting environment is controlled via GCOM's Azure Active Directory (AAD) tenant and is restricted to administrators. All administrative users are required to have two-factor authentication enabled, and this extends to use of command-line tools in the Azure environment, where device authorization (with two-factor authentication for the user) is also required.

A few components, such as the jump box VM, have specific credentials assigned to access them. These credentials are stored as secrets in Terraform and used when the resources are created.

Revocation of administrative rights would occur anytime a current administrative user's employment is terminated, their account is suspected to be compromised, or their status changes so that they no longer require administrative access.

For the TierPoint development environment, access is limited to US persons and is controlled by VPN. GCOM is currently transitioning the VPN from FortiClient to a Perimeter 81 Zero Trust VPN.

4.11.2 System

The system itself (including client application and API) relies on the state NCID system for authenticating users. To accomplish this, the system includes an OpenID Connect (OIDC) compliant identity management component, built on the Duende Identity Server product¹⁸. Having a separate identity provider provides several benefits:

- Security infrastructure can be centralized, which reduces the attack surface of the system as a whole
- The client application and API endpoints only have to deal with one type of authentication (OIDC), and this is handled by the identity management component
- We can leverage security best practices by using a robust and widely used tool (Identity Server) for the identity management component
- We can isolate authentication changes or additions to the identity provider component (for example, supporting additional forms of federated authentication) without making any downstream changes to the client application or API

¹⁸ For more information on Identity Server, see: <https://duendesoftware.com/products/identityserver>

The following diagram shows the interaction flow between the client app/end user, the identity management system (labeled as “Identity SP” in the diagram) and NCID (labeled as “SAML IdP”):

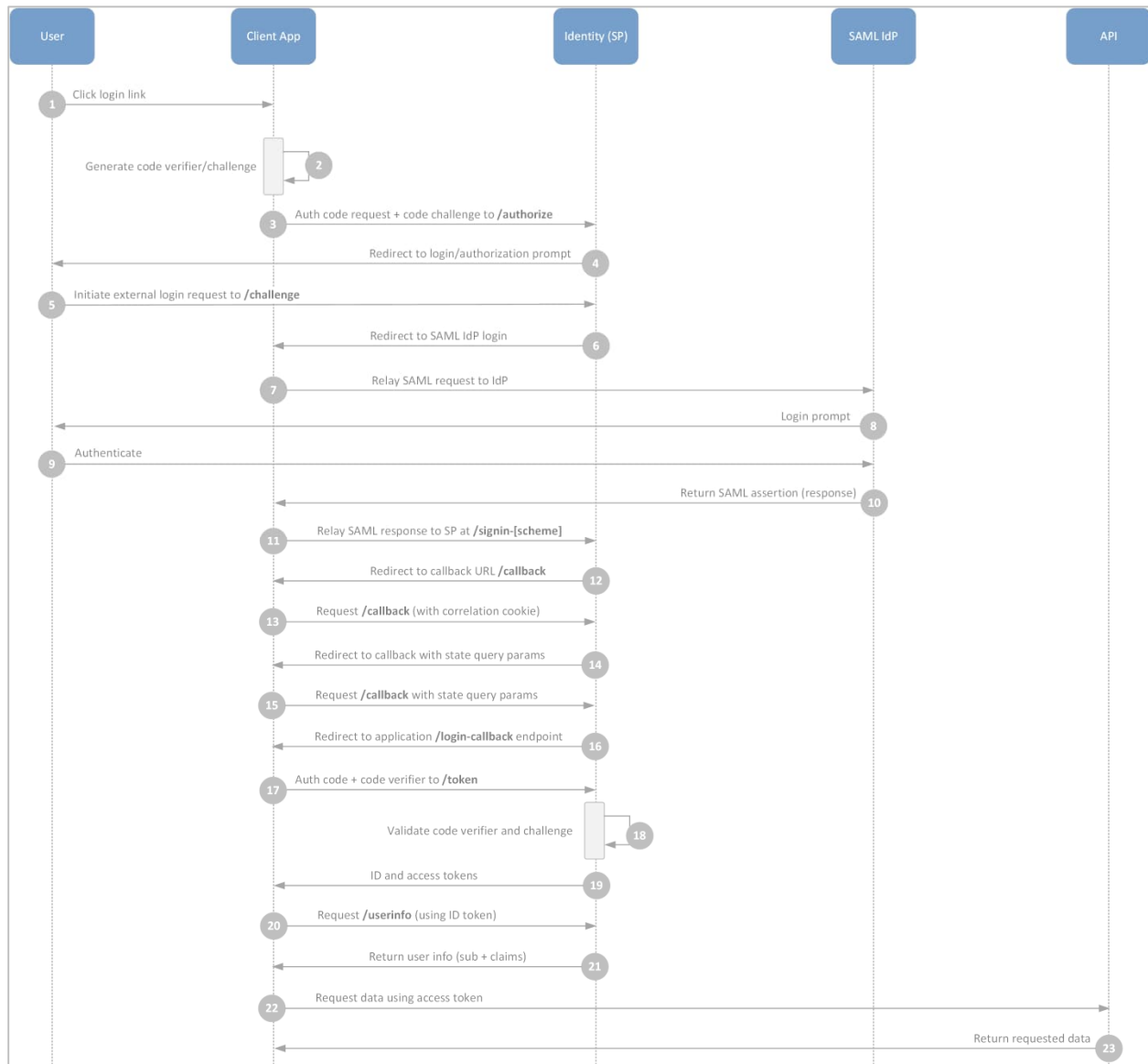


Figure 5: Interaction Flow

4.11.3 Auditing

Since NCID is the identity provider (where users enter credentials and login), the CACFP system does not record login attempts directly. NCID is responsible for auditing successful and failed logins and would retain those records. For example, if a user incorrectly entered their password, only NCID would have that information.

However, once the user has successfully logged into NCID and is redirected to the CACFP system, additional log records will be created indicating they have logged in successfully. For first-time users (with a valid NCID, but new to the system), their account creation in the identity management component and profile creation in the API will be recorded. Both the identity management

component and the API track user activity by user ID, which is correlated to the NCID-provided identity directly.

4.11.4 Profiles

Because the system does not maintain user accounts, it includes an onboarding workflow where new external accounts (from NCID) are vetted and approved by authorized program staff. The system will prompt new users who have successfully signed in using NCID to create a profile in the system. Profile requests for both internal employees and external users (such as end users working at institutions served by the program) are reviewed and approved before access is granted. Once users have a profile linked to their NCID identity, they will be taken to the appropriate area of the system.

4.12 Application Security Controls

After users log into the system via NCID and the identity management component, the system provides granular access controls. Users are assigned to roles, and roles are assigned sets of fine-grained permissions. Each API endpoint evaluates the current user's permissions to determine if they have rights to perform the requested action. Since every call to the API requires these checks, user permissions are cached at the API level for a short time to reduce the number of database lookups needed. However, for sensitive endpoints tied to administrative functions, including modifications to user accounts or roles/permissions, user state and permissions are evaluated per-request to avoid any issues from stale cache data.

Permissions are grouped into sets for assignment to roles. Permission sets are tied to modules and programs in the system. Therefore, the permission sets assigned to a user control which modules they have access to. The schema for this data is shown in the diagram below:

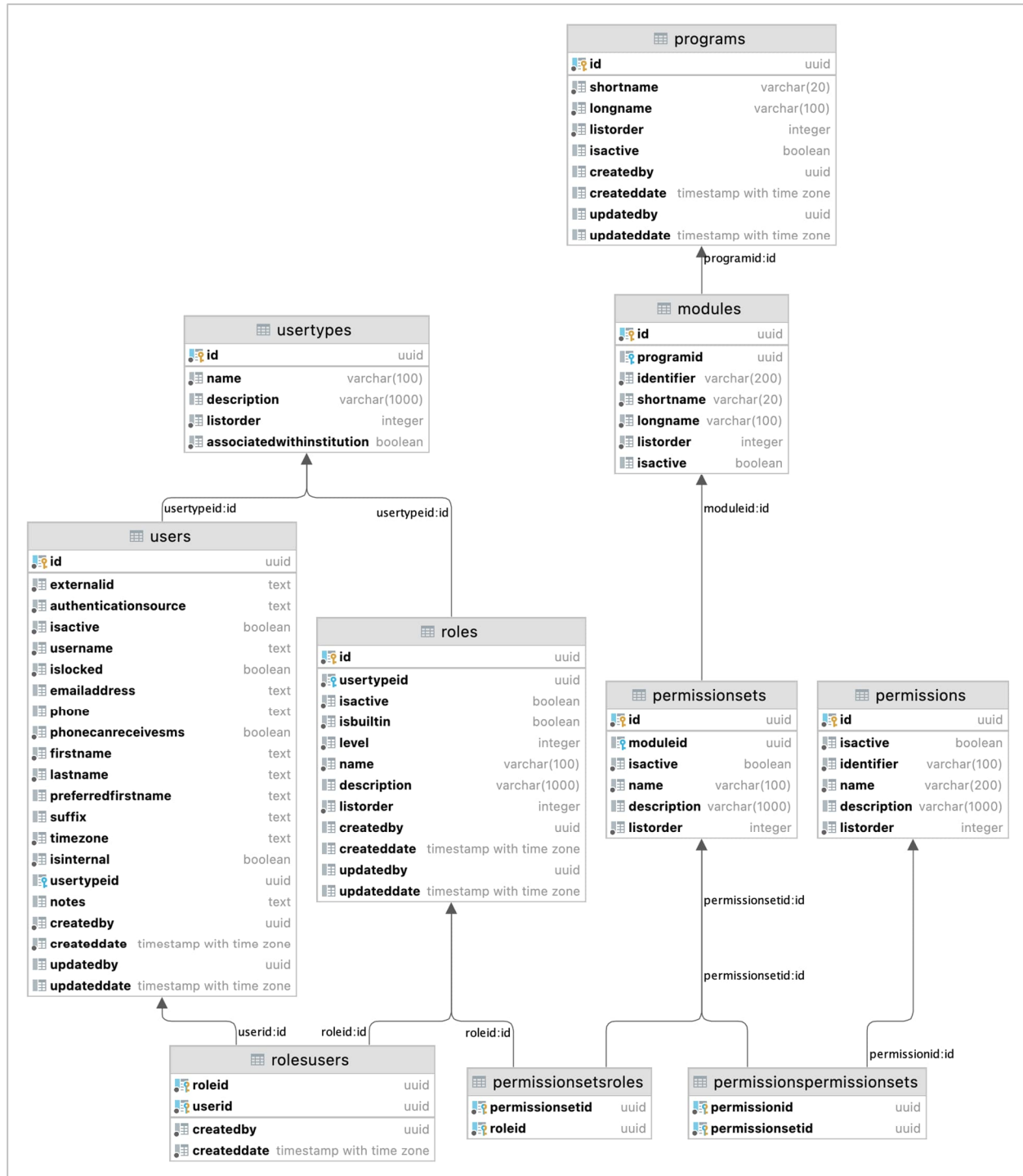


Figure 6: Permission Sets Schema

4.13 Remote Access

Remote access refers to the ability of operations personnel to connect to and inspect various system components to evaluate system health or to troubleshoot problems. There are two types of remote access enabled in the system:

- Access to a jump box VM deployed alongside the components, in the private VNet
- Access to the AKS control plane

4.13.1 Jump Box

The jump box is a virtual machine (VM) that is in a subnet inside the main VNet. Its purpose is to provide an entry point in the network for operations users to “jump” to other components. Some examples of activities that these users might perform:

- Connecting to the database to run queries or update data manually
- Connecting to the Redis instance to inspect or modify cache entries
- SSH into a pod or container instance to inspect files on the file system

By centralizing this type of access to a jump box, the attack surface of the system is greatly reduced. The jump box is only accessible to approved users and can only be connected to via the Azure Bastion service. Bastion is tied into AAD, which makes it easy to manage or revoke access by user. All AAD users must authenticate with two-factor authentication, and access to Bastion will be restricted to hardened administrative accounts.

4.13.2 AKS Control Plane

As mentioned above in the section Containers and Orchestration, the AKS control plane is vital to secure. AKS allows for IP-based restrictions as to who can connect to the control plane. In addition, the AKS cluster is tied to Azure Active Directory (AAD) for role-based access control. Two-factor authentication to AAD is required for all users, and of course the correct role assignments must be made to allow users to interact with the control plan API, either at a command prompt or via the Azure portal.

4.14 Development Practices

The earliest step in creating a secure system is to keep the process by which the system is created secure. This means:

- Controlling who can access and modify source code
- Providing formal means for code changes to be reviewed
- Automating build processes
- Integrating with cloud hosting provider security controls when publishing build outputs for deployment

4.14.1 Access Controls

GCOM uses Azure DevOps to store the source code for the system. Azure DevOps is tightly integrated into the company's Azure Active Directory (AAD) tenant. This ensures that only authorized users and stakeholders can access the system's source code. For non-GCOM employees, accounts are made in the GCOM AAD so that access can be managed in the same way for all users.

4.14.2 Code Review

Source code is stored using the Git source control system, and this allows us to use pull requests to manage changes to the system. Major source code changes are summarized in pull requests which are then reviewed and approved by senior developers/team leads. This allows senior team members to catch any security issues early.

4.14.3 Automated Build Processes

To “build” the system is to take the source code it is written in and compile it into a format that is suitable for deployment. GCOM only uses automated processes to build the system. This eliminates human error as a vector for mistakes or omissions and ensures that security guidelines put in place during the build process are consistently applied. The current build process has the following steps:

- Set an idempotent build number that is never reused (helpful later to know exactly which version is being deployed, and the chain of custody for that version from the original build)
- Compile the code from source
- Run unit tests on the compiled code
- Create database deployment change scripts
- Build the deployable containers
- Publish the containers to a private container registry in Azure, using generated machine credentials to ensure that there is a clear chain of custody for later deployments

4.15 Deployment Processes

Deployment is the work of getting the built application components out to the cloud hosting provider and ready for use. GCOM plans to automate all aspects of deployments. Automated deployments eliminate human error as a source of issues, and they keep all the target environments as uniform as possible. Having consistent environments means that we can be confident that builds deployed to test environments will function identically in production environments.

4.15.1 Environment Preparation

Setting up the cloud hosting provider to be ready to host application components is a very complex undertaking. With the highly segmented physical architecture that the system uses, there are

hundreds of different parts that need to be created and configured across all the environments. Trying to set up these components manually is a recipe for disaster because the environment is too complex for a human to remember over time.

GCOM uses a platform called Terraform to manage the complexity of building and deploying environments¹⁹. Terraform is an infrastructure-as-code tool, which means that all the components and their configuration in the cloud can be described in a code-like language. This takes knowledge and understanding of the deployment environments out of the hands of individuals and documents it in a way that dev team and operations personnel can share and understand. For example, this is the code that defines the Redis cache implementation in Azure for the development environment:

```
resource "azurerm_redis_cache" "dev-cache" {
  name                = var.redis_cache_name
  location            = azurerm_resource_group.dev-rg.location
  resource_group_name = azurerm_resource_group.dev-rg.name
  capacity            = var.redis_cache_capacity
  family              = var.redis_cache_family
  sku_name            = var.redis_cache_sku
  redis_version       = var.redis_cache_version
  enable_non_ssl_port = var.redis_cache_enable_non_ssl
  minimum_tls_version = var.redis_cache_minimum_tls_version
  public_network_access_enabled = false
  redis_configuration {
  } |
  tags = {
    env = var.tag_environment_name
    team = var.tag_team_name
  }
}
```

Note that many of the key settings start with “var.” This means that the actual value is stored in a variable (in a separate file). This makes the configuration highly flexible, because all the key configuration attributes can be specified with defaults and even overridden at deployment time. For example, the production environment cache server might be larger or use a premium SKU. This can be accomplished easily when setting up environment-specific deployments.

Some settings about the environment are sensitive. These are set up with placeholders in variables; the variable content is supplied at runtime from Terraform. Only select employees have access to Terraform so that sensitive information is kept safe.

¹⁹ For an introduction to how Terraform works, see:

<https://learn.hashicorp.com/tutorials/terraform/infrastructure-as-code>

The Terraform tool does more than just the initial deployment. It can evaluate the defined configuration and validate that the cloud environment has not drifted from the specification. This is very useful for ensuring that environments are standardized. Terraform keeps track of the complete state of the deployment and it will create, delete, or modify resources as needed to meet the specification. The following screenshot shows the result of a recent deployment (with some changes) to a development environment:

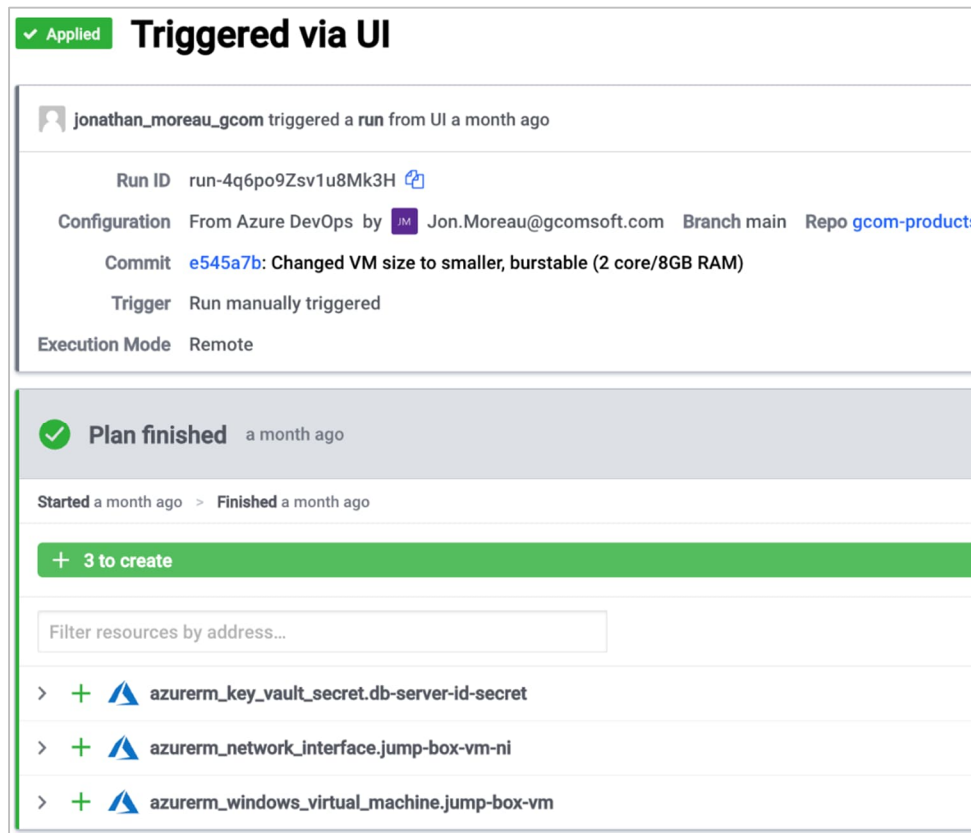


Figure 7: Terraform Tool Sample Illustration

Note how the screenshot shows who made the change, and which commit in source control triggered the deployment, in addition to showing which changes were made. This means there is always a chain of custody for any infrastructure changes. Leveraging source control branching and merging practices allow for this process to be completely automated.

4.15.2 Scope of Responsibilities

The development team is responsible for deployments to development and test environments. GCOM's managed services team will handle deployments to production environments. Using the same automated tools for all deployments will ensure quality and consistency.

4.16 Instrumentation, Logging, and Telemetry

4.16.1 Instrumentation

The system provides a full set of metrics for each system component. These metrics are provided in Prometheus format, which is a common industry standard for instrumentation. In addition to typical performance metrics, such as CPU and memory utilization, the components also expose usage metrics via the same endpoint. These include metrics like average call times, numbers of requests to each endpoint, and number of errors or failures. Every endpoint in the component has specific metrics published for it, and endpoints are generalized so that the same calls with different data can be grouped together for reporting. These metrics can be consumed by a wide variety of other tools and then used to create graphs over time. This allows operations personnel to see how the system is performing and to recognize anomalies.

The following image shows some sample CPU metrics collected using Prometheus and visualized using Grafana (the actual tools used in test and production environments may vary—the screenshot is from a development environment):

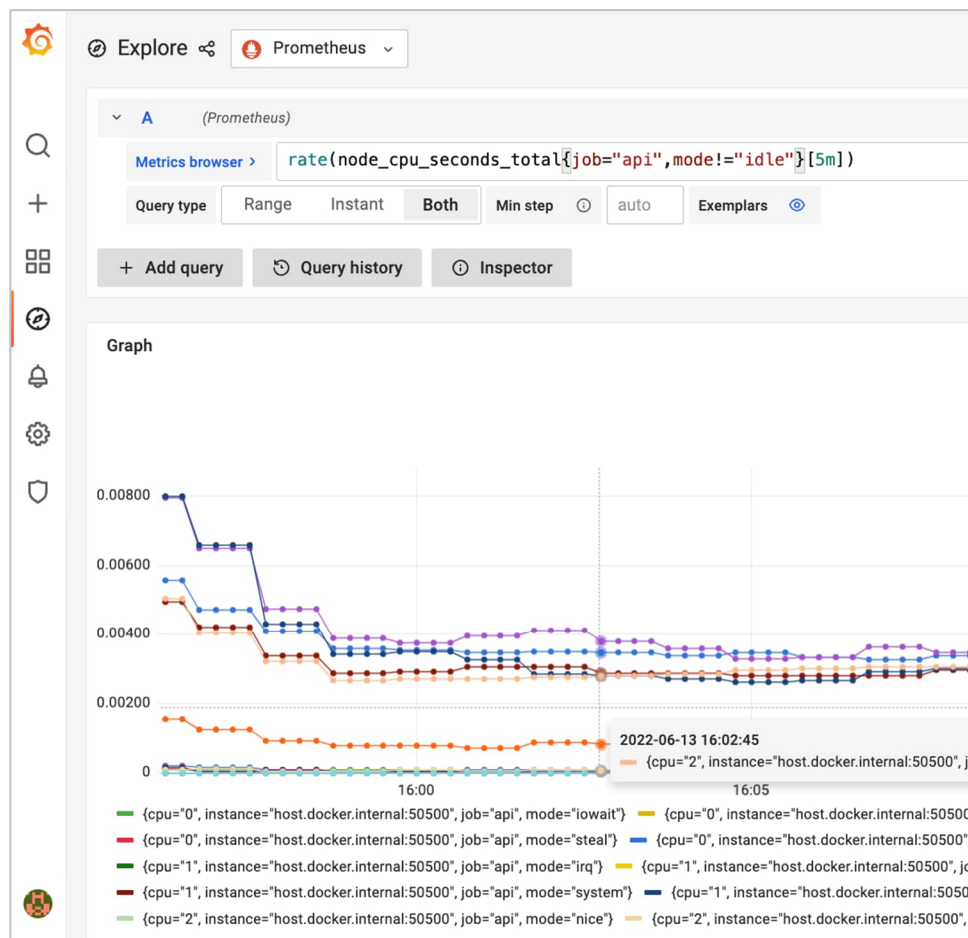


Figure 8: sample CPU metrics

4.16.2 Logging

4.16.2.1 Log Event Sources and Aggregation

When deployed and running in a cloud environment, the system consists of at least four different containers for back-end services: API, identity management, real-time communication, and background workers. Each type of container will usually have at least 2 running instances, meaning at a minimum there will be 10 containers running to support the application. In addition, the container orchestrator creates and destroys container instances as needed, which means containers are transient and do not have a long lifetime. For this reason, all logging is done to a centralized logging sink.

4.16.2.2 Structured Logging

Log events are not stored only as text. For most log messages, a template is used for the message text. For example, a login event might include the text, "User with ID '00000000-0000-0000-0000-000000000001' logged in successfully." When this log message is created, the ID in the text is sent as a parameter to the logging sink. This allows for querying by parameter later. This type of logging is called "structured logging"²⁰. The following diagram shows detail for a single log entry with the structured logging parameter shown at the bottom:

timestamp [UTC]	operation_id	message
6/10/2022, 8:09:34.403 ...	f8b13ccb0bde9fdf9b42d73c6c70e...	Fetching counties for state with identifier "00000000-0000-0000-0000-000000000001"
timestamp [UTC]	2022-06-10T20:09:34.403Z	
operation_id	f8b13ccb0bde9fdf9b42d73c6c70e281	
message	Fetching counties for state with identifier "00000000-0000-0000-0000-000000000042"	
severityLevel	0	
itemType	trace	
customDimensions	{"RequestPath":"/api/lookup/states/00000000-0000-0000-0000-000000000042/counties"	
ActionId	d11d17e4-9b54-4ff4-8f38-3bae84f729ca	
ActionName	Gcom.Cnmpis.Api.Controllers.Lookup.LookupController.GetCounties_v1 (Gcom.Cnmpis.Api)	
ConnectionId	0HMIAPDR30BA1	
MessageTemplate	Fetching counties for state with identifier {StateIdentifier}	
ParentId	a28ead140b147ffb	
RequestId	0HMIAPDR30BA1:0000000A	
RequestPath	/api/lookup/states/00000000-0000-0000-0000-000000000042/counties	
Scope	["LookupController.GetStates_v1"]	
SourceContext	Gcom.Cnmpis.Api.Controllers.Lookup.LookupController	
SpanId	7558d7e4cd1619b6	
StateIdentifier	00000000-0000-0000-0000-000000000042	
TraceId	f8b13ccb0bde9fdf9b42d73c6c70e261	

Figure 9: Structured Logging Example

²⁰ For more information about structured logging, see the following article on microservice logging best practices; look for the section "Structured Logging": <https://docs.microsoft.com/en-us/azure/architecture/example-scenario/logging/unified-logging>

4.16.2.3 Log Correlation

As described in more detail in the Telemetry section, requests to the system API are correlated under a transaction ID. This includes log messages, and it allows log events to be queried by the parent transaction. This helps when troubleshooting because related log messages can be view together as a group.

The following diagram shows an example of a query in Application Insights showing several log messages correlated under a single transaction ID:

4.16.2.4 Log Storage

In the Azure cloud hosting environment, log messages are sent to Application Insights for storage. This allows operations personnel to view and search through log messages from every component when troubleshooting. The Azure Kubernetes Service (AKS) environment has its own logging functionality and also logs message centrally to a log analytics workspace instance associated with the cluster.

4.16.3 Telemetry

The system captures telemetry data for all operations on the API. This telemetry data captures a nested view of the activities associated with each operation, starting with the inbound HTTP request, and going down to the lowest level of code execution. The OpenTelemetry standard is used to maximize interoperability with different types of log stores.

The following diagram shows some example telemetry data captured from a call to the API by Application Insights. Some items to note:

- The calls are nested and include timestamps and durations, all in the context of the operation ID. Log messages are correlated against this same operation ID, so that they can be associated with the telemetry data for more detailed troubleshooting.
- The code component responsible for the work is clearly identified, which helps developers see which paths through code were exercised (this example shows that the user and permissions were fetched from cache rather than the database, for instance).

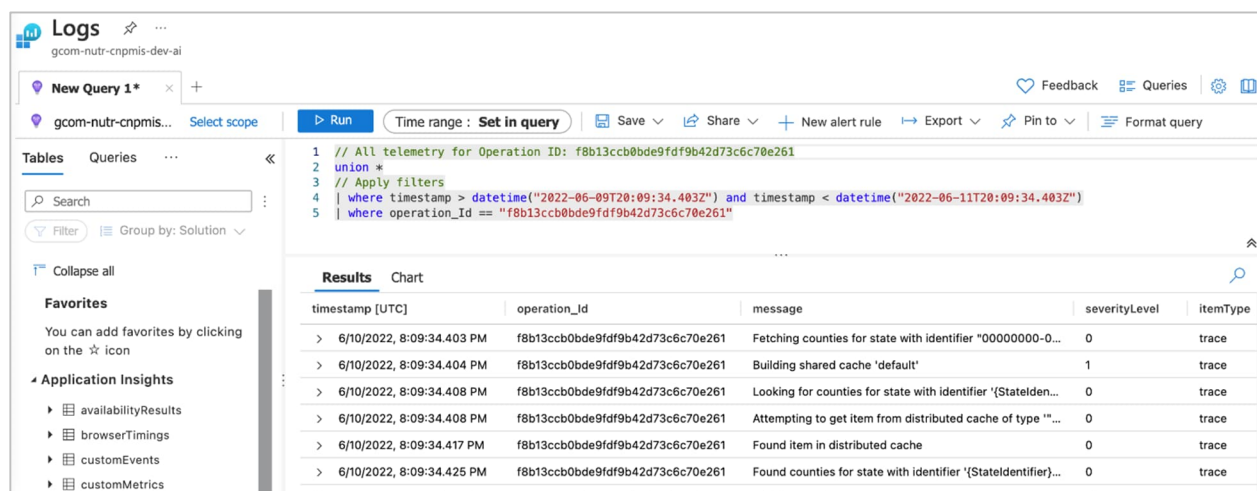


Figure 10: Application Insights Query Example

4.17 Vulnerability Assessments and Mitigation

The CACFP team will also employ automated security scans using the dynamic application security testing tool WebInspect, developed by Micro Focus, to ensure that all the appropriate security countermeasures are properly configured²¹. WebInspect evaluates and reports for all major compliance regulations related to web application security including:

- PCI DSS
- DISA STIG
- NIST 800-53
- ISO 27K
- OWASP
- HIPAA

WebInspect additionally tracks client-side frameworks that can become vulnerabilities and provides reporting on necessary upgrades to meet DevOps needs.

The state may perform additional black box application vulnerability scans and infrastructure vulnerability scans per state policies. Any application vulnerability issues will be shared with GCOM for evaluation.

GCOM will support annual penetration testing per CA-8 policy and will work with program staff to determine which party will perform annual testing.

²¹ For more detail on WebInspect's capabilities, see this whitepaper:
https://www.microfocus.com/media/data-sheet/webinspect_automated_dynamic_application_security_testing_ds.pdf

Appendix H: Risks and Issues Management Plan

The following pages provide NC WIC the Risk and Issues Management Plan which describes the approach to managing risk and issues for the North Carolina Crossroads Maintenance and Enhancement project.



Crossroads MIS
Maintenance and Enhancement Services

North Carolina WIC Program

Appendix H
Risks and Issues Management Plan

Trademarks

Trademarked names may appear throughout this document. Rather than list the names and entities that own the trademarks or insert a trademark symbol with each mention of the trademarked name, the names are used only for editorial purposes and to the benefit of the trademark owner with no intention of infringing upon that trademark.

Contact Information

To request copies, suggest changes, or submit corrections, contact:

North Carolina Department of Health and Human Services**Division of Child and Family Well-being, WIC Program**

Attention: Molly Jones

Crossroads WIC Release Manager

Phone: 252-903-3951

Email: Molly.Jones@dhhs.nc.gov

Revision History

Date	Version	Revised By	Description
12/18/2018	0.1	Jay Saunders, Three Sigma Software	Draft version
3/6/2025	1.0	Jennifer Saunders, Voyatek	Submission for RFP 30-25002-DCFW

Deliverable Description

This Risk and Issues Management Plan describes the approach to managing risk and issues for the North Carolina Crossroads Maintenance and Enhancement project.

Table of Contents

1. Introduction	1
2. Risk Management Approach	2
3. Roles and Responsibilities	4
4. Risk Identification.....	6
5. Risk Prioritization and Characterization	7
6. Risk Response Planning	8
7. Risk Monitoring, Controlling, and Reporting.....	9

Table of Figures

Figure 1: Risk Governance	2
Figure 2: Prioritization.....	7

Table of Tables

Table 1: Roles and Responsibilities	4

1. Introduction

A risk is an event or condition that, if it occurs, could have a negative effect on a project's objectives. The purpose of the Risk and Issues Management Plan for North Carolina WIC is to establish the framework in which the project team will identify risks and develop strategies to mitigate or avoid those risks. This plan also defines how risks associated with the project will be recorded, and monitored throughout the lifecycle of the project.

This Risk and Issues Management Plan includes the following sections:

- Risk Management Approach – Deciding how to approach and conduct the risk management activities for the project
- Roles & Responsibilities – Defining how each team role contributes to managing the risk process
- Risk Identification – An initial and continuous effort to identify, quantify and document risks as they are identified.
- Risk Prioritization & Categorization – Evaluate identified risks to determine probability of occurrence, impact, and timeframe.
- Risk Response Planning - Establish an action plan for risk and assign responsibility.
- Risk Monitoring, Controlling, & Reporting – Capture, compile, and report risk using the Risk Register

2. Risk Management Approach

The basic Risk Management approach for NC WIC is to identify critical risks and take necessary action before issues arise that impact project objectives. Many different tools will be used as part of this strategy.

The approach taken to manage risks for this project will include a methodical process by which the project team will identify, score, and rank various risks. Risk information identified by the project team will be entered into the Risk Register. The Product Manager will maintain the Risk Register, and Risk information will be a principal topic in all NC WIC status meetings. New risks will be reviewed to determine if mitigation action is required. The most likely and highest impact risks will be added to the project plan to ensure that the assigned risk managers take the necessary steps to implement the mitigation response at the appropriate time during the project. Risk managers will provide status updates on their assigned risks in weekly project team meetings, but only when the meetings include their risk's planned timeframe. Upon completion of the project, during the closing process, the Product Manager will analyze each risk and review the risk management process. Based on this analysis, the Product Manager will identify any improvements that can be made to the risk management process for future projects. These improvements will be captured as part of the lessons learned knowledge base.

The risk management strategy we employ provides an overall view of the project's risks and allows the project team and stakeholders to take intelligent actions to decrease, mitigate, and eliminate risks. A collaborative approach to risk management is critical to anticipate, identify, and mitigate project risks. We include State stakeholders in all risk management processes. Our team's risk management approach (depicted in the figure to the right) facilitates risk identification, tracking, and mitigation of project risks from all relevant stakeholders.

We employ a risk management approach that is proactive, collaborative, and integrated into our overall project management toolset. To leverage the tools used on other projects, we propose to use Microsoft (MS) SharePoint along with Team Foundation Server as our primary tool. Key tenets of our approach follow.



Figure 1: Risk Governance

- **Governance** – Identify the institutions, plans, and actions by which the authority for risk and issue management is exercised and decisions are taken and implemented.
- **Identification** – Collaborate with the State office, local Women, Infants, and Children (WIC) agencies, Department of Information Technology, Electronic Benefit Transfer (EBT) Project staff, and our team to identify and document risks and issues which may impact progress or system operations.
- **Analysis** – Evaluate risks and issues for characteristic categories, and quantify on a numerical scale according to probability, impact, and level of control for risks, and type and priority for issues.
- **Planning** – Collaborate to develop options and determine actions that could mitigate each risk and resolve issues.

- **Implement Mitigation Strategy/Escalate** – Execute decisions and mitigation action plans for each risk and escalate as issues persist.
- **Monitor Risks and Issues** – Work with the State WIC office, Department of IT, EBT vendor, and other stakeholders to correct deviations from planned risk actions, and monitor action status to resolve issues.

3. Roles and Responsibilities

The table below provides an overview of the Roles & Responsibilities for the NC WIC Risk Management activities.

Table 1: Roles and Responsibilities

Role	Responsibilities
Business Analysts	Assists in identifying and determining the context, consequence, impact, timing, and priority of the risk
Product Manager	- Chairs the risk assessment meetings - Coordinates with Risk Managers to determine if the risk is unique - Identifies risk interdependencies across projects and verifies if risk is internal or external to project - Assigns risk classification and tracking number - Continually monitors the projects for potential risks throughout the project lifecycle - Analyzes any new risks that are identified and add these items to the Risk Register
Risk Manager	- Coordinates with the Product Manager to identify the risks, the dependencies of the risk within the project, and the context and consequence of the risk - Determines the impact, timing, and priority of the risk - Formulates the risk statements - Monitors and controls risks that have been identified - Reviews and updates the top ten risk list [timeframe, as needed, every two weeks, etc.] - Escalates issues & problems to management
Risk Owners	- Determines which risks require mitigation and contingency plans - Generates the risk mitigation and contingency strategies and performs a cost benefit analysis of the proposed strategies - Monitors, controls, and updates the status of the risk throughout the project lifecycle - Aids in the development of the risk response and risk trigger - Carries out the execution of the risk response if a risk event occurs - Participates in the review, re-evaluation, and modification of the probability and impact for each risk item on a weekly basis - Identifies and participates in the analysis of any new risks that occur - Escalates issues/problems to PM that significantly impact the projects triple constraint or trigger another risk event to occur - Highlights risks that require action prior to the next weekly review - Identifies and escalates risks where strategy is not effective or productive (causing the need to execute the contingency plan)

Role	Responsibilities
Other Key Stakeholders	Assists in identifying and determining the context, consequence, impact, timing, and priority of the risk

4. Risk Identification

Risk identification will involve the project team, and appropriate stakeholders, and will include an evaluation of environmental factors, organizational culture and the project management plan including the project scope, schedule, cost, or quality. Careful attention will be given to the project deliverables, assumptions, constraints, Work Breakdown Schedule, cost/effort estimates, resource plan, and other key project documents.

The following methods will be used to assist in the identification of risks associated with NC WIC:

- Expert Interviews
- Risk Assessment Meetings
- Historical Reviews of Similar Projects
- Brainstorming
- Interviewing
- SWOT (Strengths, Weaknesses, Opportunities and Threats)
- Diagramming

The Risk Register will be updated as needed and will be stored electronically in the project library located at the project Sharepoint site.

5. Risk Prioritization and Characterization

In order to determine the severity of the risks identified by the team, a probability and impact factor will be assigned to each risk. This process will allow the Product Manager to prioritize risks based upon the potential impact to the project.

As risks are assigned a probability and impact, the Product Manager will move forward with risk mitigation/avoidance planning.

The probability and impact of occurrence for each identified risk will be assessed by the Product Manager, with input from the project team using the following approach:

Probability:

- High – Between 80% and 100% probability of occurrence
- Medium – Between 20% and 79% probability of occurrence
- Low – Below 20% probability of occurrence

Impact:

- High – Risk that has the potential to greatly impact project cost, project schedule or performance
- Medium – Risk that has the potential to slightly impact project cost, project schedule or performance
- Low – Risk that has relatively little impact on cost, schedule or performance

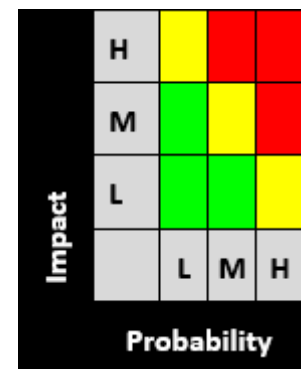


Figure 2: Prioritization

Risks that fall within the RED and YELLOW zones will have a risk response plan which may include both a risk response strategy and a risk contingency plan.

6. Risk Response Planning

Each major risk (those falling in the Red & Yellow zones) will be assigned to a risk owner for monitoring and controlling purposes to ensure that the risk will be addressed and managed appropriately.

For each major risk, one of the following approaches will be selected:

- **Avoid** – Eliminate the threat or condition, or avoid impact to the project objectives by eliminating the cause. The project plan may need to be altered to account for the risk avoidance. Avoidance may be achieved by changing scope, adding time, or adding resources.
- **Mitigate** – Identify ways to reduce the probability or the impact of the risk. These steps may be costly and time-consuming, but could be preferable to allowing the risk to go forward in an unmitigated state.
- **Accept** – The project team accepts that the risk exists and makes no change to the project plan to address the risk. No response strategy is identified.
- **Contingency** – Define actions to be taken in response to risks.
- **Transfer** – Shift the consequence and ownership of a risk by making another party responsible (buy insurance, outsourcing, etc.).

The Product Manager will lead the project team in developing responses to each identified risk. As more risks are identified, they will be qualified and the team will develop the response. These risks will also be added to the Risk Register and the project plan to ensure they are monitored at the appropriate times and are responded to accordingly.

For each risk that will be mitigated, the project team will identify ways to prevent the risk from occurring or reduce its impact or probability of occurring. This may include prototyping, adding tasks to the project schedule, adding resources, etc. Any secondary risks that result from risk mitigation responses will be documented and will follow the same risk management protocol as primary risks.

7. Risk Monitoring, Controlling, and Reporting

The Risk Register for NC WIC is a log of all identified risks, their probability and impact to the project, the category they belong to, mitigation strategy, and when the risk is estimated to occur. This register will be created in the early planning phase of the project. Based on the identified risks and timeframes in the risk register, applicable risks will be added to the project plan. At the appropriate time in the plan—prior to when the risk is most likely to occur—the Product Manager will assign a risk manager to ensure adherence to the agreed upon mitigation strategy.

The level of risk on NC WIC will be tracked, monitored, controlled and reported throughout the project lifecycle. The most likely and greatest impact risks will be added to the project schedule to ensure that proper monitoring occurs during the time of risk exposure. As risks are added to the project schedule, a Risk Manager will be assigned. During the weekly project team meeting, the Risk Manager will discuss the status of their assigned risks. Only risks which fall in the current time period will be discussed. Risk monitoring will be a continuous process throughout the life of this project.

Critical risks will also be assigned a risk owner(s) who will track, monitor, and control their assigned risks. The risk owner will also provide a weekly status report to the Product Manager and Risk Management Team. This report should contain an assessment of the effectiveness of each risk response action.

As Risk Events occur, the list will be re-prioritized during weekly reviews and the risk management plan will reflect any and all changes to the risk lists including secondary and residual risks.

The Product Manager will notify the Crossroads WIC Release Manager of important changes to risk status as in the weekly Project Status meeting and monthly Project Status report.

Appendix J: Configuration Management / Release Management Plan

The Configuration Management / Release Management Plan below describes the approach to the Voyatek team will take in managing the configuration of the Crossroads system and providing ongoing releases of the system during the North Carolina Crossroads Maintenance and Enhancement project.



Crossroads MIS
Maintenance and Enhancement Services

North Carolina WIC Program

Appendix J
Configuration and Release Management
Plan

Trademarks

Trademarked names may appear throughout this document. Rather than list the names and entities that own the trademarks or insert a trademark symbol with each mention of the trademarked name, the names are used only for editorial purposes and to the benefit of the trademark owner with no intention of infringing upon that trademark.

Contact Information

To request copies, suggest changes, or submit corrections, contact:

North Carolina Department of Health and Human Services**Division of Child and Family Well-being, WIC Program**

Attention: Molly Jones

Crossroads WIC Release Manager

Phone: 252-903-3951

Email: Molly.Jones@dhhs.nc.gov

Revision History

Date	Version	Revised By	Description
12/18/2018	0.1	Jay Saunders, Three Sigma Software	Draft version
3/6/2025	1.0	Jennifer Saunders, Voyatek	Submission for RFP 30-25002-DCFW

Deliverable Description

This Configuration and Release Management Plan describes processes for managing Crossroads system configuration, version control for release source code, release management processes, and coordination with the EBT vendor for the North Carolina Crossroads Maintenance and Enhancement project.

Contents

1	Vendor Procedures	1
1.1	Configuration Documentation	1
1.2	Document Version Control.....	2
1.3	Source Code Version Control	4
1.4	Automated Deployments	4
1.5	Test Scripts	5
2	Release Management Process	7
2.1	Process Overview	7
2.2	Version Control	8
2.3	Release Numbering	11
2.4	Concurrent Release Support.....	13

Figures

Figure 1: SharePoint Portal.....	3
Figure 2: Version History	3
Figure 3: Sample test script form	6
Figure 4: Test evidence example.....	7
Figure 5: Visual Team Studio & Azure DevOps Integration Illustration.....	8
Figure 6: Illustration of Source control branching.....	9
Figure 7: Example Crossroads Change History	10
Figure 8: Management of Multiple Releases Illustration	10
Figure 9: Sample Crossroads change history for the MyNCWIC portal	11
Figure 10: Version Labels.....	12
Figure 11: Release Archive.....	13
Figure 12: Changeset Details Screen.....	13

1 Vendor Procedures

1.1 Configuration Documentation

Voyatek assumed responsibility for all existing configuration documentation and work for North Carolina during our initial contract. This plan describes our standard of practice for maintaining documentation and configuration. Voyatek maintains configuration data for a variety of business and technical configuration components. These include:

System Settings

Voyatek maintains a spreadsheet based “notebook” of all system configuration settings found within the user interface. Each value is stored with the appropriate setting label on tabs that represent configuration of user interfaces within Crossroads. While this process is time consuming, it allows for testing that the system is configured as intended and ensures that UAT/Test/Training environments are configured to match production settings (or non-production settings as appropriate.)

This process is primarily helpful during the implementation phase of MIS projects but can be a valuable tool for ongoing management. System Settings spreadsheets are saved in SharePoint with version control enabled to allow for the tracking of changes over time.

Cross-Reference Table

Voyatek received the set of spreadsheets with tabs for each user interface and columns for all “drop-down” or user definable values from the previous M&E vendor. These documents define selections for configurable questionnaires/surveys and other functions. These spreadsheets were tied to quality assurance test scripts to confirm environment configuration and to test interactions between configured values that interact with business logic. Configuration values that have embedded business logic were noted within configuration documents and provided reference for future changes as to potential impacts of those changes.

During the course of our contract, NC deemed that the maintenance of these spreadsheets no longer provided sufficient value that warranted the amount of effort needed to make these updates. Should a configuration change be necessary, such changes are documented as part of Change Requests and other documentation as appropriate. Additionally, when NC needs to review or analyze existing configuration, whether for an enhancement or any other reason, Voyatek will export the configuration data, all or data only related to the specific need, and provide it to NC.

Web.config Files

Web.Config and other server configuration data is stored within source control to allow for the tracking of versions.

IIS/Server Settings

IIS/Server Settings is documented as an appendix to system setup and configuration documentation or within a separate reference document. Sensitive information including passwords and encryption keys is excluded from configuration documentation.

Other Configuration Data

In addition to the items above, Voyatek also maintains documentation for several specialized data sets within WIC systems. These are typically larger sets of configuration data with specialized maintenance needs. The primary example of these types of customized configuration documents would be:

- Risk Codes
- Food Category and Subcategory Setup
- Approved Foods List

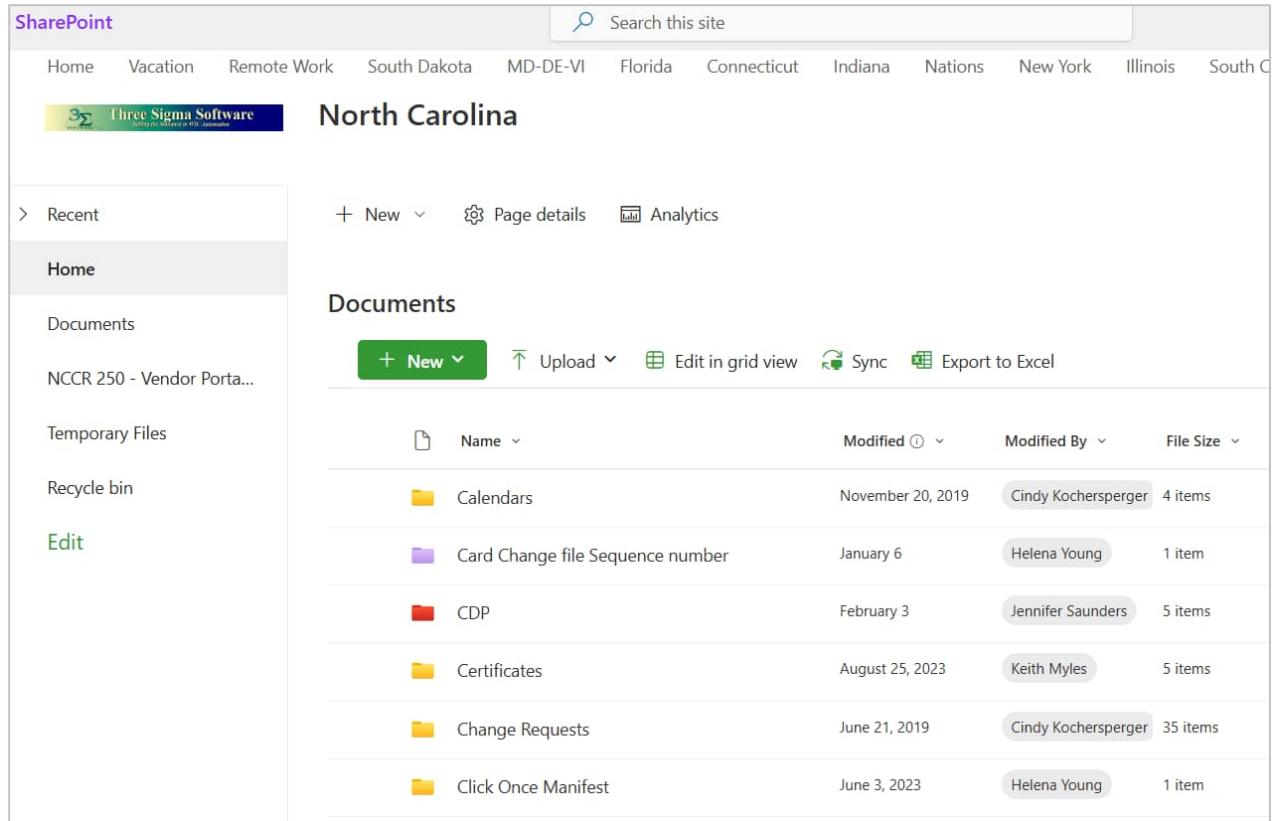
Configuration values with more extensive business rule documentation or with large volumes of data are typically maintained in separate customized documents. Approved foods lists are generally managed in an external tool rather than within a traditional configuration document.

1.2 Document Version Control

Each document will contain a section for Version History. This history will maintain a version number, author name, and date for each document update. Voyatek staff responsible for document updates will be trained to update this information as part of each update. Key project staff are familiar with Crossroads documentation and version management. This is also the standard for all Voyatek projects.

In addition to maintaining version history within documents, Voyatek utilizes Microsoft SharePoint to track all document changes. North Carolina will receive access to a dedicated private SharePoint folder where all project documents will be located. Voyatek will provide authorized North Carolina direct access to the SharePoint site. If the user already has a Microsoft 365 account, they will be able to use the same login/password to the Voyatek portal.

SharePoint offers a variety of helpful features. Users can download documents, upload documents, follow documents to be notified of changes, share documents, edit documents from within their web browser, and share links to documents instead of emailing them directly. Documentation will be organized in a folder structure to allow for organization of files to meet North Carolina's needs. A sample of the SharePoint portal is shown below:



SharePoint

Search this site

Home Vacation Remote Work South Dakota MD-DE-VI Florida Connecticut Indiana Nations New York Illinois South C

Three Sigma Software

North Carolina

+ New Page details Analytics

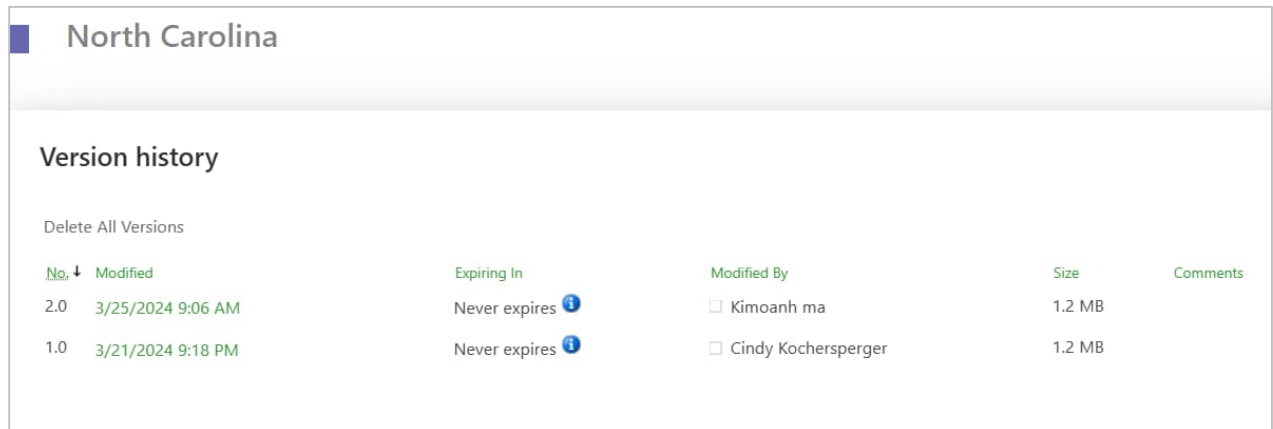
Documents

+ New Upload Edit in grid view Sync Export to Excel

Name	Modified	Modified By	File Size
Calendars	November 20, 2019	Cindy Kochersperger	4 items
Card Change file Sequence number	January 6	Helena Young	1 item
CDP	February 3	Jennifer Saunders	5 items
Certificates	August 25, 2023	Keith Myles	5 items
Change Requests	June 21, 2019	Cindy Kochersperger	35 items
Click Once Manifest	June 3, 2023	Helena Young	1 item

Figure 1: SharePoint Portal

The SharePoint portal maintains a full editing history for all document changes. This feature allows users to view prior versions, identify when changes have been made, and to recover lost content in the case of error. A sample of the Version History appears below:



North Carolina

Version history

Delete All Versions

No.	Modified	Expiring In	Modified By	Size	Comments
2.0	3/25/2024 9:06 AM	Never expires	Kimoanh ma	1.2 MB	
1.0	3/21/2024 9:18 PM	Never expires	Cindy Kochersperger	1.2 MB	

Figure 2: Version History

As needed, SharePoint can also serve as a repository for release notes, release installation packages, and other project materials.

1.3 Source Code Version Control

Microsoft Azure DevOps (DevOps) is used for storing Crossroads source code and building application components for publishing and deployment. Source code changes are tracked using Git and tagged to DevOps work items allowing users to view both the change and build history from a common location.

DevOps is integrated into Microsoft Visual Studio to allow developers to check-out and check-in source code seamlessly while performing development tasks. Code is checked in as a changeset linked to issues, changes and tasks maintained within DevOps. The DevOps tools are also integrated to support the generation of deployable code from any DevOps version control branch (software release). This is designed to prevent the introduction of unwanted source code or the failure to deploy desired code in a release. The complete details of TFS Version Control are provided later in this documentation.

1.4 Automated Deployments

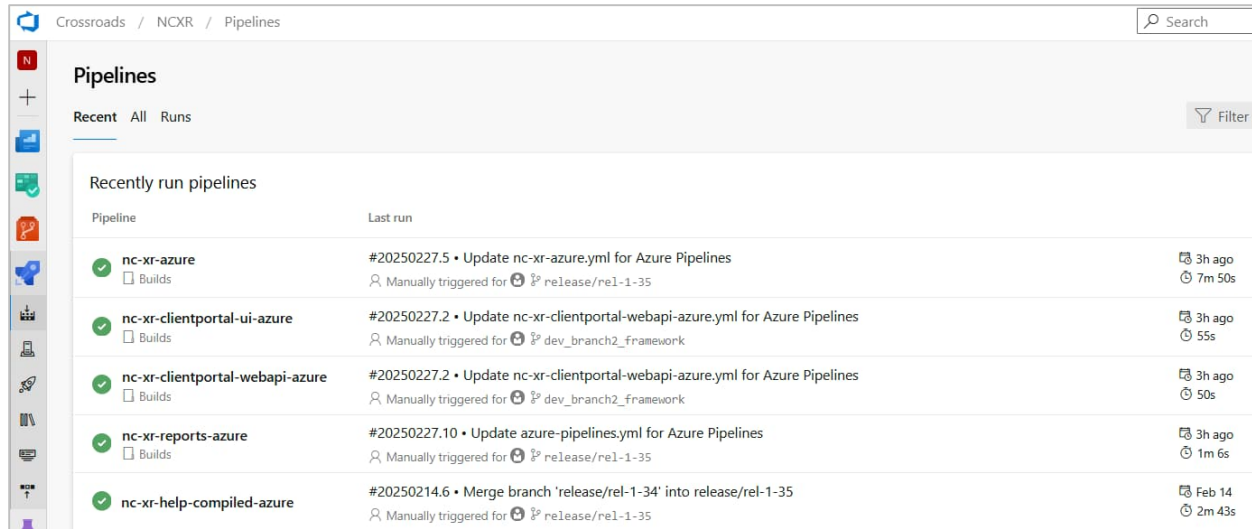
Deployment automation starts in DevOps, which stores source code and manages the build process. Automating deployment includes the following steps:

- Retrieving source code from a code branch based on the targeted release version
- Compiling the code into executable form
- Running unit tests
- Linking code changes in the release to work items such as user stories and bugs
- Creating deployment packages from compiled code that are published to environments
- Publishing build results and linked work items

Once the code is built, Voyatek utilizes the Octopus Deploy platform for deploying Crossroads code to environments. Octopus uses the same process for all environments, which keeps them consistent with one another and makes environment management and troubleshooting much easier. Octopus stores environment configuration settings separately from the deployment process. Each environment has its own settings for database connection strings, file locations, and other configurable system data. Where there are minor differences in environments, the deployment path can be branched to accommodate these.

We also require progressive deployment of code to hosting environments. For example, code cannot be deployed to production without first being deployed to lower test and UAT environments. This prevents code differences between environments while ensuring that code is tested before being promoted to higher environments.

Database deployments, such as schema changes and data updates, are also handled by Octopus. Developers write script changes separately and in a defined order. Octopus then applies these changes in the target environment. A list of what scripts have been run in each database is used to determine which ones need to be executed as part of a deployment. This allows the process to work against any environment, bringing it up to date, whether deployments have been done recently or not. The figure below shows a recently run release pipeline from the automated deployment software for NC Crossroads.



The screenshot shows the 'Pipelines' section in Azure DevOps for the 'Crossroads / NCXR' project. It displays a list of recently run pipelines under the 'Recent' tab. The table includes columns for Pipeline, Last run, and a search/filter icon. The pipelines listed are:

Pipeline	Last run	Time
nc-xr-azure Builds	#20250227.5 • Update nc-xr-azure.yml for Azure Pipelines Manually triggered for release/rel-1-35	3h ago 7m 50s
nc-xr-clientportal-ui-azure Builds	#20250227.2 • Update nc-xr-clientportal-webapi-azure.yml for Azure Pipelines Manually triggered for dev_branch2_framework	3h ago 55s
nc-xr-clientportal-webapi-azure Builds	#20250227.2 • Update nc-xr-clientportal-webapi-azure.yml for Azure Pipelines Manually triggered for dev_branch2_framework	3h ago 50s
nc-xr-reports-azure Builds	#20250227.10 • Update azure-pipelines.yml for Azure Pipelines Manually triggered for release/rel-1-35	3h ago 1m 6s
nc-xr-help-compiled-azure	#20250214.6 • Merge branch 'release/rel-1-34' into release/rel-1-35 Manually triggered for release/rel-1-35	Feb 14 2m 43s

Figure 8: Pipelines – Recently run pipelines for Crossroads

Once releases are approved for deployment, the automated processes work together to publish them to the hosting environment quickly and reliably, eliminating human error and applying security guidelines consistently. Our automated deployment approach has reduced the need for extensive UAT testing of system infrastructure and makes system upgrades as seamless as possible. This reliability facilitates more agile release processes with a faster release cadence, which helped the state to respond quickly to such events as FNS policy changes, formula shortages, and the COVID19 pandemic.

1.5 Test Scripts

Voyatek test scripts will be maintained in versioned Microsoft Word and/or Excel documents. Test script documents and Test Evidence will be attached to DevOps work items. Attaching test evidence to DevOps items helps when needing to research the history of specific changes or bug fixes. These can be stored within the North Carolina SharePoint site as well.

Following is a screen shot of an example of a test script in Excel showing just the beginning steps of the script to illustrate the detailed format. In this example, the script itself is 180 rows long with additional supporting screenshots of the test results. The scripts are detailed and thorough, which is essential to test and track the results for a system with the complexity of Crossroads.

NCCR- 253 Inventory Improvement - TFS 285												
EXECUTION PURPOSE		Change Request NCCR 253										
EXECUTION DETAILS		Inventory Improvement										
Tester		Helena Young										
TFS Bug #		NCCR 253										
Execution Date		10/10/2022										
Release #		1.29										
Environment Name		XRTEST										
Environment Version		1.29.22278.1										
Environment URL		Crossroads Standalone XRTEST										
TEST DATA		F00200000294										
TEST CASE STATUS												
Total # of Cases		98										
% Complete		100%										
P = Passed		98										
F = Failed		0										
B = Blocked		0										
N = Not Executed		0										
DATE CREATED	TYPE	PRIORITY	STATUS	TEST CASE #	TEST CASE DESCRIPTION	EXPECTED RESULT	SCREEN NUMBER	SCREEN SHOT	TFS Bug	Comment	Environment	
9/7/2022			P	NCCR 253_1.1	1.1 Breast Pump Issuance Process Improvements			Screenshot				
					PREREQUISITES:	1. User has all Crossroads Permissions 2. User has Crossroads Test Database Access 4. User is assigned to at least 1 Clinic location 5. Data - Active Breastfeeding Participant with issued EBT Card, Serialized Products, Unserialized Products						
					#	Description	Expected Result	Screen Number	Screen shot	TFS Bug	Comment	Environment
9/7/2022			P	NCCR 253_1.1	1	Login into Crossroads/Operations /Setup/ Maintain Breastpump Issuance questions	Operations /Setup/ Maintain Breastpump Issuance questions are displayed	10001	Screenshot			
9/7/2022			P	NCCR 253_1.1	2	Navigate to Manage Breast Pump Issuance Questions screen. Verify the Manage Breast Pump Issuance questions are inactive (uncheck the Active checkbox) displays (False)	Manage Breast Pump Issuance questions are Inactive - (False)	60087	Screenshot			

Figure 3: Sample test script form

Following is a screen shot depicting how test results evidence can be stored in MS Word following the execution of a test.

Online Version 1.28.22214.1 10109

TFS 605 - Scheduling module functionality: appointment method – Test result – PASS

Test Evidence

Clinic Master Calendar

1. Select a family and schedule a new appointment in the Clinic Master Calendar
2. Verify screen displays, title - **Appointment Method**
3. Verify the Appointment
4. Method drop down displays, **Clinic, Telephone, Video Conference**

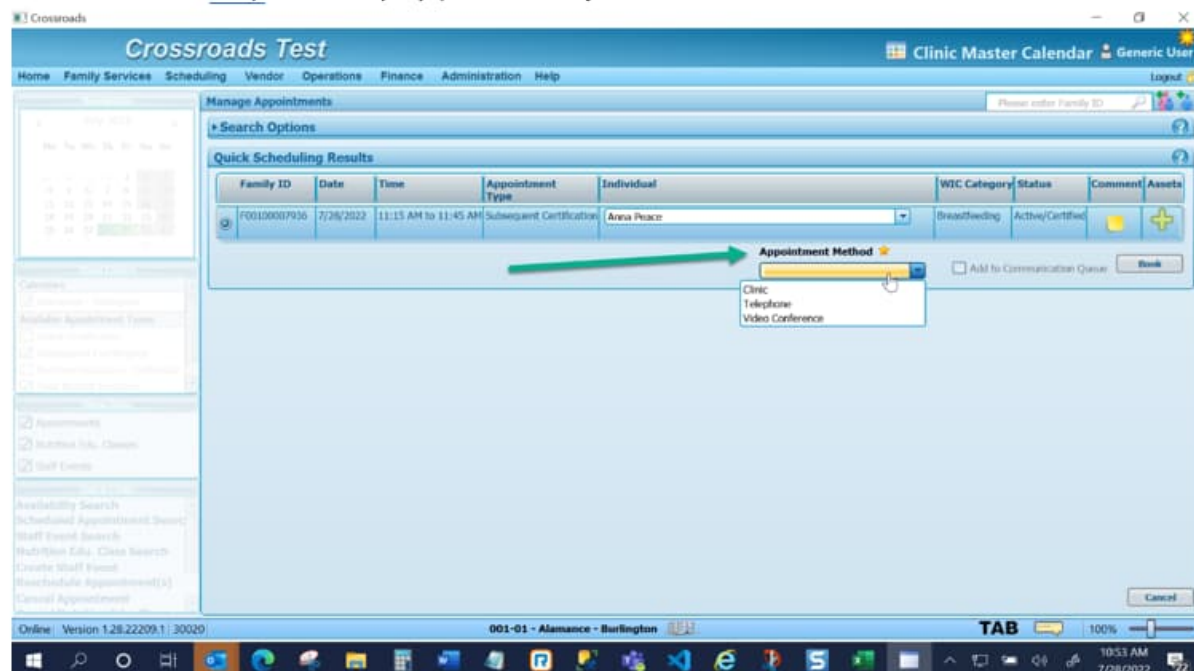


Figure 4: Test evidence example

2 Release Management Process

2.1 Process Overview

Voyatek uses DevOps and Visual Studio as an integrated suite of tools for development, source control, version control, and build control management. By using an integrated tool set, Voyatek improves the quality of releases through isolated code branching, controlled branch merging, automated builds, and process standardization.

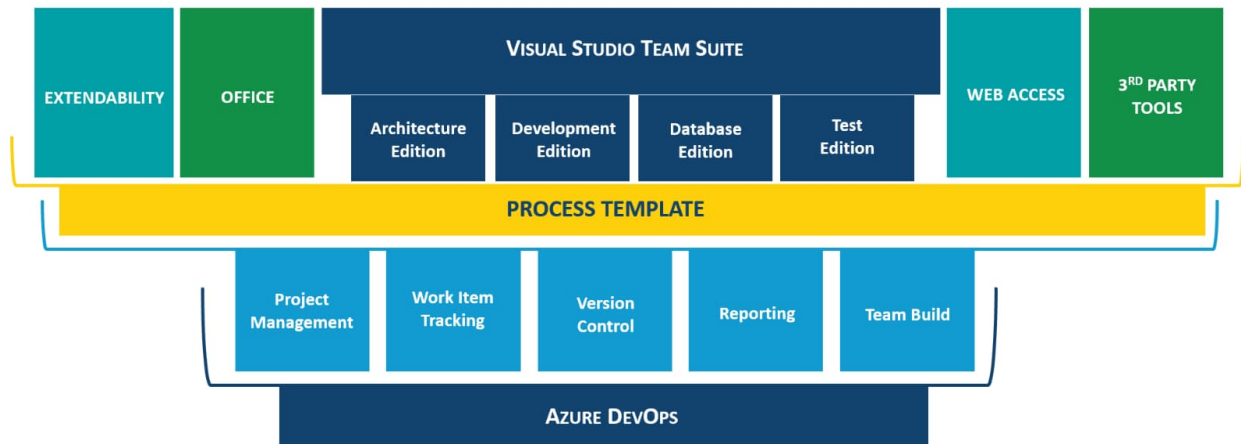


Figure 5: Visual Team Studio & Azure DevOps Integration Illustration

The distributed version control system provided by Git provides developers much better control on code management by providing a more powerful and flexible capability for branching and merging code changes wherein each developer can select precisely what is branched and merged where DevOps does it at a team level. Git branches are lightweight, and developers can quickly and efficiently switch contexts across locally created branches to pivot among the various versions of the codebase they may be working on. Also, developers have the flexibility of working on “feature branches” which allow multiple teams to work simultaneously on defect fixes and multiple enhancements without compromising the efficiency of the team. Git’s visual tools for merging and publishing branches provide a powerful capability that allows development teams to better control release content as events occur that shape the scope of the release (for example, change control board decisions about release content).

2.2 Version Control

Version control (also known as revision control or source control) is a category of processes and tools designed to keep track of multiple different versions of software, content, documents, hardware specifications and other information in development. Any system that provides change tracking and control over programming source code or documentation can be considered version control software.

Effective version control can only be achieved if the right tools and procedures are used while developing or modifying content. Be it code or documents, the degree to which the versioning of an artifact needs to be tracked will depend on the type of artifact.

Any effective version control software should provide the following features at a minimum:

- Provide a database to store configuration items that need to be version controlled.
- Allow for controlled updates (“check-ins) of configuration items that are under version control.
- Assign a unique number to each update so that the update can be identified
- Allow viewing history of updates to a controlled item
- Compare versions of a controlled item to identify changes that have happened to it over time

- Allow for “linking” related controlled items to form a baseline
- Assign a unique number to a baseline or a release

DevOps provides teams with the ability to create “branches” in the system code that allow for the numbering and identification of production releases and interim releases as part of the preparation of the next production release. In the sample below, Version 1 could represent a production release (e.g., Crossroads 1.14.0.0) and Version 2 could represent the next release (e.g., Crossroads 1.15.0.0). As the development team prepares for Release 1.16, they can create new branches for UAT deployments (Crossroads 1.16.0.0), patch releases (1.16.1.0) and other versions as development progresses.

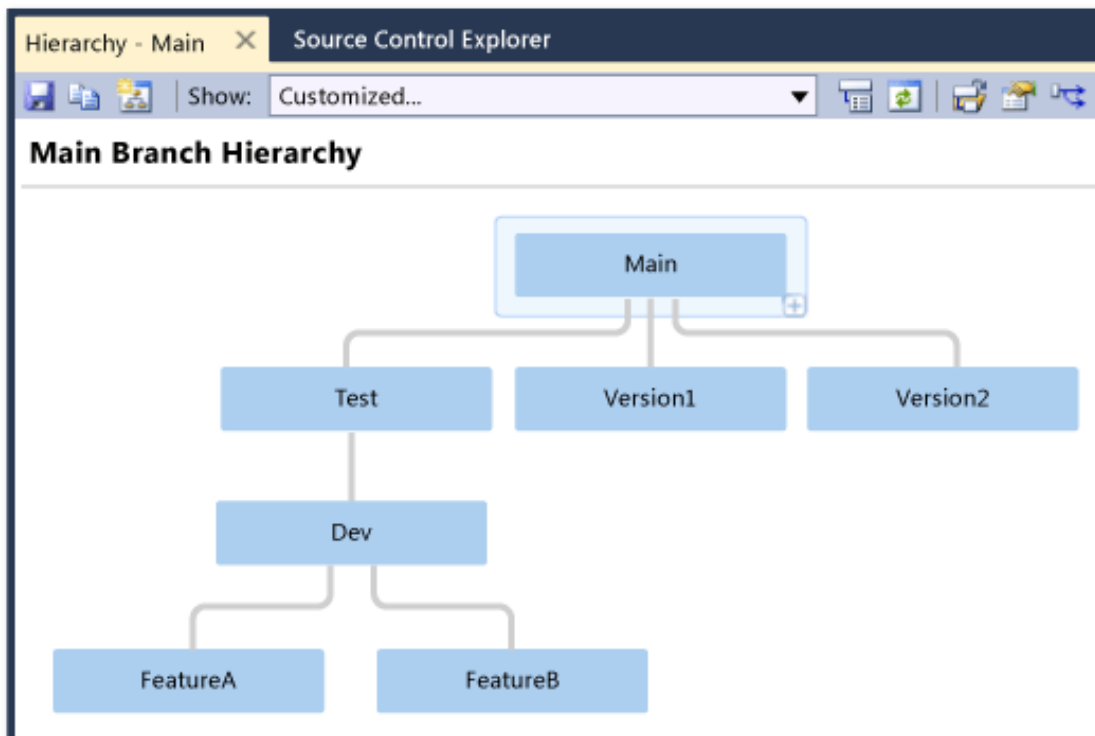


Figure 6: Illustration of Source control branching

When a branch is created in DevOps, all code associated with that software is retained in a copy. This branch can then be used to reload a release with a modification like a hot fix or to merge into the release a fix that has been prepared in a separate branch.

Developers can make changes in any code branch. When changes are ready to be checked in, a “changeset” is created. Developers are required to document notes associated with the code change and to link DevOps issue management tickets to allow for the tracking of all changes against reported issues and approved changes. Changesets can be viewed with details of when the changes occurred, and the responsible developer as shown below:

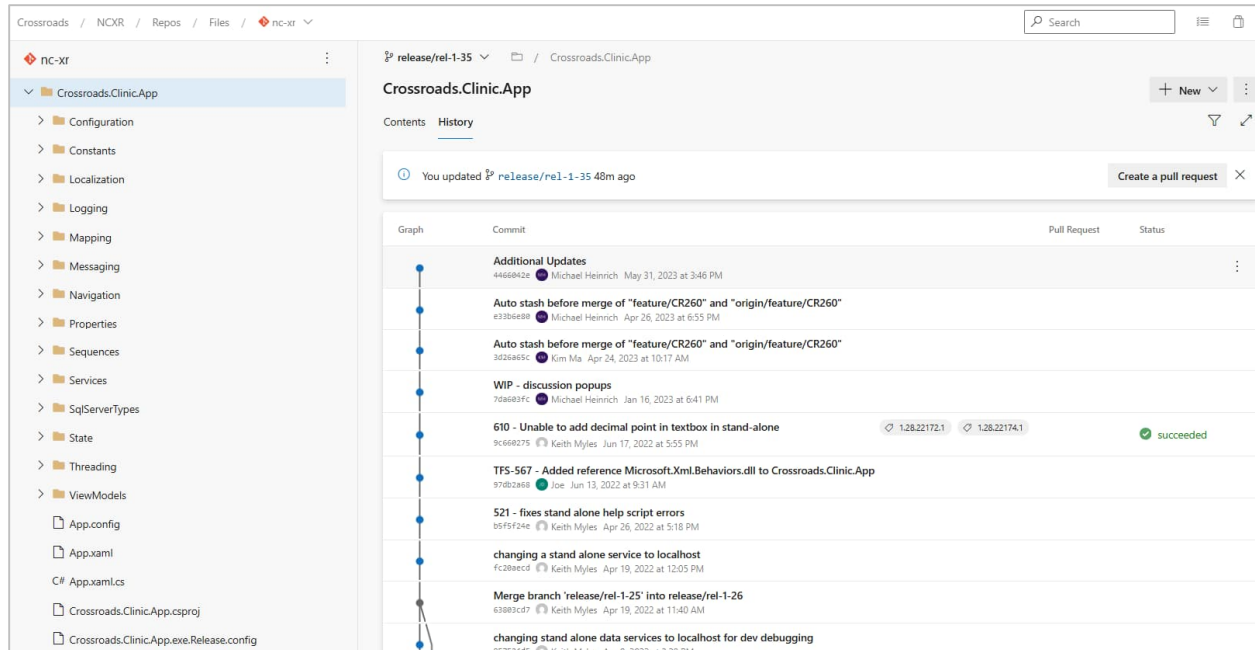


Figure 7: Example Crossroads Change History

The diagram below illustrates how Microsoft visualizes the ability to patch the current release (grey line) while developing a future release using agile sprints (blue line) and combining the two so that no changes are lost when new releases are moved to production. Changes can be moved from a hot fix into the future release (reverse integration) or moved from the future release into production to allow a targeted change to be delivered as a hot fix (forward integration.) The use of Changesets to check in each software change, allows Voyatek to add or remove specific functional changes without introducing unintended changes in the release.

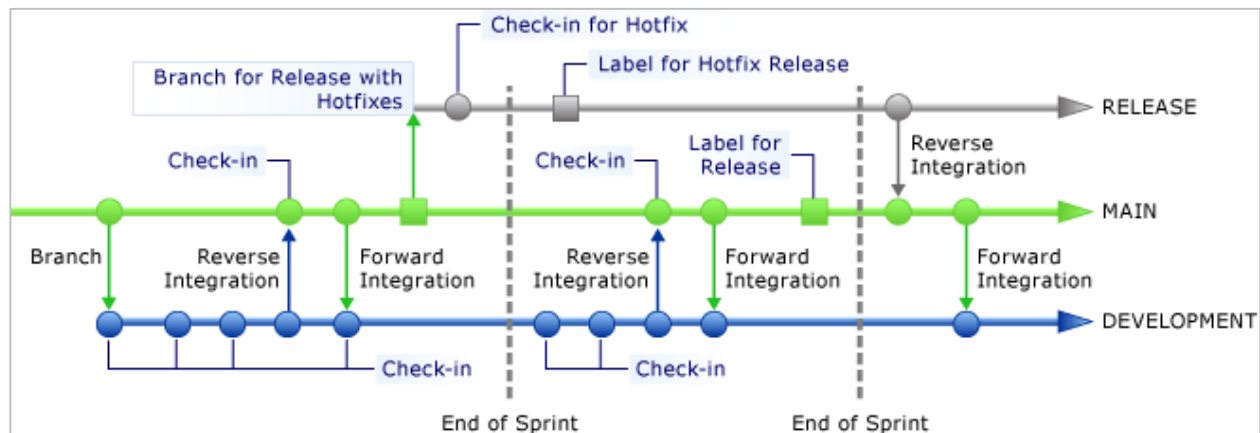


Figure 8: Management of Multiple Releases Illustration

DevOps and Git provide developers with integrated tools for merging changes from one branch to another. Performing these tasks within Visual Studio (the developers' "workbench") and DevOps

reduces the likelihood of mistakes and process failures. A sample of the merge history is shown below:

Pull Requests			
	Created by	Assigned to	Pull request ID
Mine	Active	Completed	Abandoned
	Merge spotu_dev to dev_branch2_framework Sreenivasa Potu requested #44 into  dev_branch2_framework		11/7
	Test push Anthony Acaldo requested #41 into  master_framework_integrated		9/2
	Merge dev_branch_UX to dev_branch2 Anthony Acaldo requested #38 into  dev_branch2		9/7
	Merge dev_branch2 to master Anthony Acaldo requested #37 into  master		9/7
	Merge dev_branch_UX to dev_branch2 Anthony Acaldo requested #36 into  dev_branch2		9/7
	Merge dev_branch2 to master Anthony Acaldo requested #33 into  master		9/7
	Merge dev_branch_UX to dev_branch2 Anthony Acaldo requested #31 into  dev_branch2		9/7
	Merge TeleHealth_KM3 to branches/development Kimoanh Ma requested #28 into  branches/development		9/7
	Merge TeleHealth_KM3 to branches/development Kimoanh Ma requested #27 into  branches/development		9/7

Figure 9: Sample Crossroads change history for the MyNCWIC portal

2.3 Release Numbering

Release identification numbers help identify the version of the release in an environment. Voyatek will maintain the release numbering methodology requested by North Carolina.

The use of 4 version numbers is standard for all Microsoft development. DevOps branch management allows Voyatek to create code branches labelled to match the standards outlined by North Carolina.

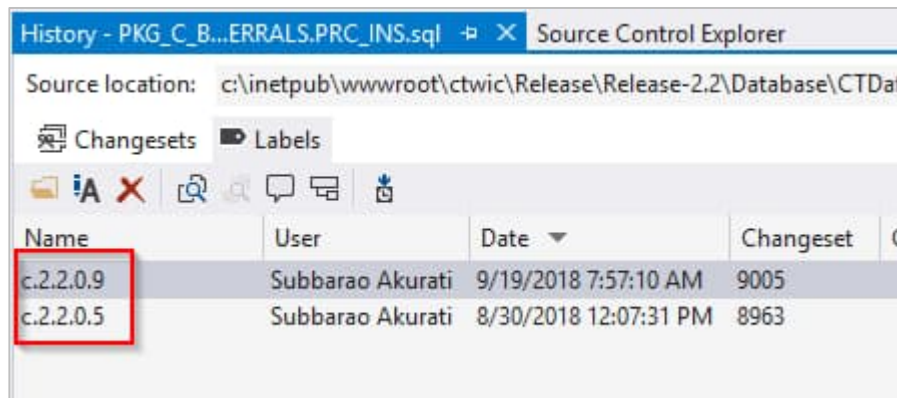
Voyatek typically follows a 4-digit numbering system for releases as described below.

1. **Platform Release** – This is the first digit of the release and denotes the generation release number. The generation release number is incremented when there is a fundamental change to the application, for example an addition of a new feature or a technology upgrade that makes the application significantly different from its current state.
2. **Major Release** – This is the second digit of the release and denotes the major release number. The major release number is incremented during regular upgrades to the system that do not warrant a platform release number change. Generally, post-production, Voyatek schedules quarterly releases to promote bug fixes and enhancements to the system to allow for sufficient time for the design, development and verification steps. This number would be updated for each such release.

3. **Minor Release** – This is the third digit of the release and signifies a production patch. If there is a need to patch a UAT or production release, this digit would be incremented.
4. **Hot Fix / Build Number** – This is the fourth and last digit of the release number and is incremented every time a build is done to the internal testing environment. The build number will reset to 0 when either the major release or the minor release number changes.

For example, the number 1.2.1.9 denotes the 1st generation release, 2nd major release with one patch to production and 9 total builds or hot fixes. Voyatek typically uses the last digit to record each unique build to track each build that is generated more accurately allows. Crossroads currently only increments the last number when a hotfix is applied to an environment. Voyatek can utilize either approach and will configure DevOps accordingly. For clarity and consistency with Microsoft best practices, we recommend using the build based approach.

The release number also forms a “label” for code items. The “label” is initiated by the development manager based on the major and minor number of the release. In the above example, the very first label that will be assigned to code artifacts will be 1.2.1.9. When a build is released to the QA environment, all code files (.aspx, .aspx.vb, .js) and all database packages, procedure and script files will be stamped with this label number with the final label being assigned to the entire branch. The screen above shows labels that have been assigned to releases. In the sample, version numbers are prefixed with a module letter but this is not needed for Crossroads.



Name	User	Date	Changeset
c.2.2.0.9	Subbarao Akurati	9/19/2018 7:57:10 AM	9005
c.2.2.0.5	Subbarao Akurati	8/30/2018 12:07:31 PM	8963

Figure 10: Version Labels

After the build is deployed to production, the final release number is used as a label on the entire branch of the application to peg code artifacts to a release. If later, the release needs to be rebuilt, files can be extracted from DevOps using this release label and the release can be restored to the targeted version.

2.4 Concurrent Release Support

There are two primary concerns with the ability to provide concurrent release support. The first is the ability to accurately manage code from multiple releases and to create builds with the correct versions of code. Microsoft's DevOps branch management ensures that each release is immediately recoverable by any member of the team. The branch can also be compiled or built into deployable code at any time regardless of what other code is being managed by the team. These capabilities are fundamental to the DevOps tool set.

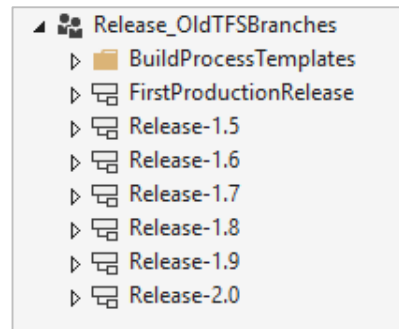


Figure 11: Release Archive

Microsoft also provides additional capabilities to assist developers in moving code between branches to improve their accuracy and to prevent errors. Some examples of these features are provided below:

- Check in tracking with notes and links to issues and tasks
- Functions to merge code including the ability to identify merge conflicts and tools for conflict resolution
- Support for reverting code changes

Below is a sample of the Changeset details screen that allows users to review one or more changes, roll them back, merge them into another branch, or perform other actions.

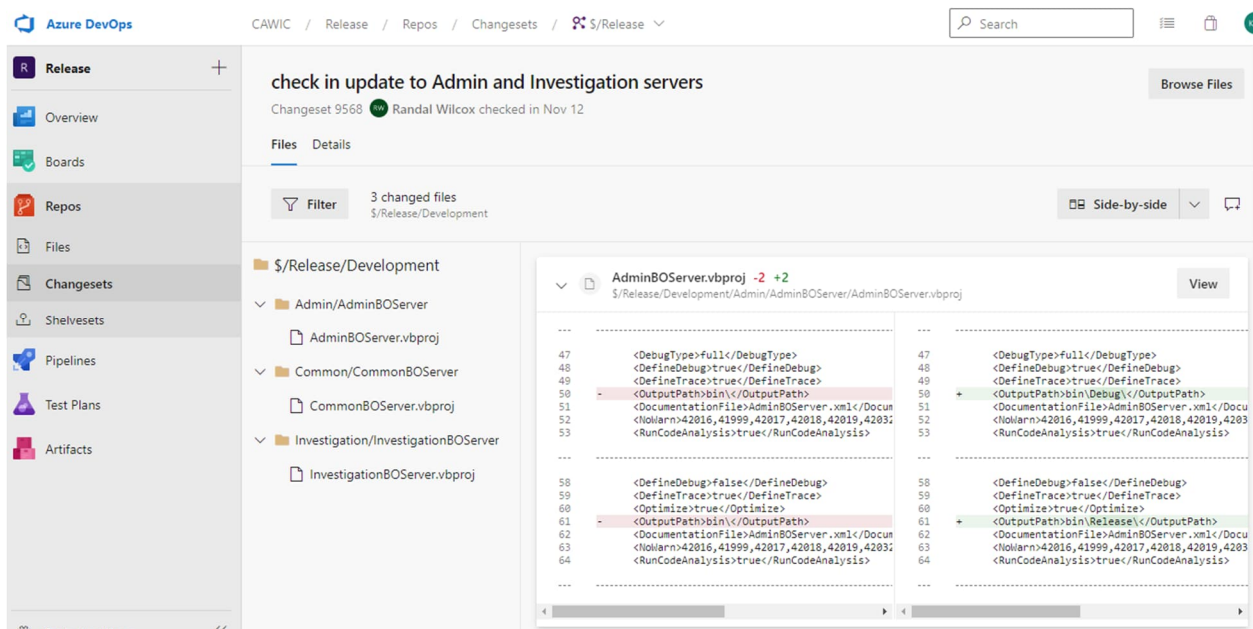


Figure 12: Changeset Details Screen

The second potential concern is having a location to deploy and test changes without interfering with other development processes. Voyatek is proposing to support a minimum of 3 internal environments to support this activity. This would include the following:

- **Development** – where future release code is developed and unit tested

- **Test** – where candidate releases are tested by quality assurance staff
- **Secondary Test** – location for testing alternative releases. This could either be a production hot fix or a long-term future system change like replacement of XBAP technology.

Support for these types of activities is a strength of Voyatek. Our team currently supports 11 major clients that each have their own development and testing environments. Voyatek always supports a combination of production, future release, and often special project release environments for our customers.

Appendix K: Evidence of Vendor Financial Stability

7.2 FINANCIAL STATEMENTS

The Vendor shall provide evidence of financial stability by returning with its offer 1) completed Financial Review Form (Attachment H), and 2) copies of Financial Statements as further described hereinbelow. As used herein, Financial Statements shall exclude tax returns and compiled statements.

a) For a publicly traded company, Financial Statements for the past three (3) fiscal years, including at a minimum, income statements, balance sheets, and statement of changes in financial position or cash flows. If three (3) years of financial statements are not available, this information shall be provided to the fullest extent possible, but not less than one year. If less than 3 years, the Vendor must explain the reason why they are not available.

b) For a privately held company, when certified audited financial statements are not prepared: a written statement from the company's certified public accountant stating the financial condition, debt-to-asset ratio for the past three (3) years and any pending actions that may affect the company's financial condition.

c) The State may, in its sole discretion, accept evidence of financial stability other than Financial Statements for the purpose of evaluating Vendors' responses to this RFP. The State reserves the right to determine whether the substitute information meets the requirements for Financial Information sufficiently to allow the State to evaluate the sufficiency of financial resources and the ability of the business to sustain performance of this RFP award. Scope Statements issued may require the submission of Financial Statements and specify the number of years to be provided, the information to be provided, and the most recent date required.

Voyatek is providing the following information for Evidence of Vendor's Financial Stability:

1. Please find the completed Financial Review Form in section a), [Attachment H – Financial Review Form](#).
2. Copies of our Financial Statements are provided below.

GCOM HoldCo LLC
GCOM Software LLC

Statement of Corporate Financial Resources

GCOM HoldCo LLC and Subsidiaries ("GCOM" or the "Company") is a company organized on October 26, 2017, under the laws of the state of Delaware. The Company was formed with the primary purpose of providing professional information technology software and services to federal, state, and local governments.

The Company's primary investor, Sagewind Capital LLC, a NY-based long-term private equity partner with over \$1.0 Billion of assets under management, and other investors have continued to support and invest in the growth of GCOM.

The following outlines GCOM's total current asset, total current liability and ratio percentage of current asset to current liability. In addition, subsequent information is provided for consideration to demonstrate financial stability.

GCOM Software LLC

	12/31/2023	12/31/2022	12/31/2021	Adjusted 12/31/2023	Adjusted 12/31/2022	Adjusted 12/31/2021
Current Assets:						
Cash	\$ 5,833,000	\$ 1,278,000	\$ 3,036,000	\$ 5,833,000	\$ 1,278,000	\$ 3,036,000
Accounts Receivable	80,149,000	44,630,000	52,378,000	80,149,000	44,630,000	52,378,000
Other Current Assets	1,839,000	2,008,000	2,099,000	1,839,000	2,008,000	2,099,000
Total Current Assets	87,821,000	47,916,000	57,513,000	87,821,000	47,916,000	57,513,000
Current Liabilities:						
Current Debt	\$ 8,300,000	\$19,680,000	\$ 3,906,000	\$ 8,300,000	\$19,680,000	\$ 3,906,000
Accounts Payable	12,947,000	6,506,000	6,170,000	12,947,000	6,506,000	6,170,000
Accrued Expenses	53,216,000	44,336,000	23,405,000	53,216,000	14,836,000	14,905,000
Other Current Liabilities	8,403,000	4,131,000	4,085,000	400,000	1,747,000	-
Total Current Liabilities	82,866,000	74,653,000	37,566,000	74,863,000	42,769,000	24,981,000
Ratio of Current Assets to Current Liabilities	1.1	0.6	1.5	1.2	1.1	2.3
Revolver Availability	\$40,000,000	\$10,000,000	\$15,000,000	\$40,000,000	\$10,000,000	\$15,000,000
Ratio of Current Assets+Revolver Availability to Current Liabilities	1.5	0.8	1.9	1.7	1.4	2.9

remove Earnout liabilities (Debt like)
remove Deferred Revenue (non Cash)

Additional considerations demonstrate financial stability:

In August 2023, GCOM completed the acquisition of OnCore Consulting. The acquisition of OnCore materially transformed GCOM, improving its overall financial position. As a result of the transaction:

- GCOM's revenues more than doubled.
- GCOM's profitability nearly tripled.
- GCOM's leverage position was reduced by over 50%.
- As part of the August 2023 acquisition, GCOM Software LLC now has access to a revolving line of credit of up to \$45,000,000.

The following shows GCOM's proforma income statement for the combined GCOM/OnCore entity from 2022 through projected 2024 financial information.

GCOM - Pro Forma Financials
(\$ in thousands)

	2021	2022	2023E	2024P
Revenue	\$ 269,153	343,090	362,870	376,010
Direct costs	182,578	227,002	240,852	247,420
Gross profit	86,575	116,088	122,019	128,590
Operating expenses	38,108	36,786	35,655	35,783
Operating income	48,467	79,302	86,363	92,806

GCOM Software LLC believes these financial results and considerations demonstrate financial stability as outlined in the Florida Statutes.

In addition to its financial strength:

1. GCOM Software LLC is well within compliance of the financial ratios required to be maintained by our credit agreements.
2. GCOM Software LLC is in good standing with all States, Cities, Federal Government, and commercial enterprises with which it does business.
3. GCOM Software LLC is in material compliance with all its contractual relationships and has no pending or threatened litigation against it.
4. GCOM Software LLC has never been sued for non-performance or had an unresolved dispute about its contractual performance.

If you would like further information about our financial ability to perform, please feel to contact Glen Marder (glen.marder@gcomsoft.com).

**Glen
Marder**

Digitally signed by Glen Marder
DN: cn=Glen Marder, o=US, ou=GCOM
Software, LLC, ou=Finance,
email=glen.marder@gcomsoft.com
Reason: I am the author of this document
Date: 2024.01.30 12:54:35 -0700

Appendix L: Transition-Out Plan

The Transition-Out Plan outlined below describes the activities during the Transition-Out Phase, during which Voyatek will assist the State and the incoming contractor for the North Carolina Crossroads Maintenance and Enhancement follow-on project.

State of North Carolina
Department of Health and Human Services
Division of Child and Family Well-Being



Crossroads MIS
Maintenance and Enhancement Services

North Carolina WIC Program

Appendix L
Transition Out Plan

Trademarks

Trademarked names may appear throughout this document. Rather than list the names and entities that own the trademarks or insert a trademark symbol with each mention of the trademarked name, the names are used only for editorial purposes and to the benefit of the trademark owner with no intention of infringing upon that trademark.

Contact Information

To request copies, suggest changes, or submit corrections, contact:

North Carolina Department of Health and Human Services**Division of Child and Family Well-being, WIC Program**

Attention: Molly Jones

Crossroads WIC Release Manager

Phone: 252-903-3951

Email: Molly.Jones@dhhs.nc.gov

Revision History

Date	Version	Revised By	Description
12/18/2018	0.1	Jay Saunders, Three Sigma Software	Draft version
3/6/2025	1.0	Jennifer Saunders, Voyatek	Submission for RFP 30-25002-DCFW

Deliverable Description

This Transition Out Plan describes the activities during the Transition Out Phase during which Voyatek will assist the State and incoming contractor for the North Carolina Crossroads Maintenance and Enhancement follow-on project.

Table of Contents

1.	Introduction	1
2.	Transition Communications.....	2
2.1	Kickoff Meeting.....	2
2.2	Technical Coordination Sessions.....	2
2.3	Change Request and Release Planning	2
3.	Transition Out Phase Documentation Deliverables	3
3.1	Transition Out Completion Report.....	3
4.	Transition Out Phase Activities	4
4.1	Transition Out Activities	4

1. Introduction

Voyatek understands the need for a smooth transition between service providers, to ensure no interruption of service to the State or the participants. In the event Voyatek is not chosen as the follow-on service provide, Voyatek will provide a smooth transition to a new Maintenance and Enhancement Services provider. This plan outlines the steps needed to migrate Crossroads source code and project artifacts into a new provider's infrastructure for providing Maintenance and Enhancement services.

2. Transition Communications

2.1 Kickoff Meeting

Voyatek will participate in the Project Kickoff meetings with the incoming contractor. Voyatek would prefer to hold this meeting as soon as possible after contract award to allow for transition activities to begin and to have the opportunity to review key project resources with North Carolina staff and the incoming contractor. The Voyatek Product Manager will coordinate with the North Carolina Release Manager and DPH management to provide any agenda input and needed written materials prior to the kickoff meeting.

2.2 Technical Coordination Sessions

Voyatek recognizes that several elements of the project including access to North Carolina data bases, access to UAT and Production hosting environments, and other support procedures involve coordinating Voyatek activities with North Carolina technical staff and the incoming contractor. Voyatek anticipates that one or more teleconference sessions to discuss and document procedures would be helpful.

2.3 Change Request and Release Planning

Voyatek anticipates that planning for the first release in the new Maintenance and Enhancement Contract will occur during the Transition In period. Voyatek will closely coordinate with North Carolina staff and the incoming contractor to facilitate this planning. Voyatek believes that these meetings will provide good opportunities to review Change Request needs, perform Joint Application Design meetings, and to coordinate release planning with North Carolina staff and incoming contractor.

3. Transition Out Phase Documentation Deliverables

3.1 Transition Out Completion Report

Voyatek will provide the final Transition Out Completion Report no later than 10 days prior to the contract end date.

During this transition out period Voyatek will identify and provide the following items no later than 10 days prior to the contract end date.

- Deliverables submitted this transition out period
- Outstanding tasks/deliverables
- Risk tracking log
- Outstanding problems, issues, and changes
- Minutes from source code and documentation walkthrough sessions
- Minutes from known defect walkthrough sessions
- Minutes from tool, hardware, and configuration walkthrough sessions that produce and install executable builds

4. Transition Out Phase Activities

4.1 Transition Out Activities

During this transition out period, Voyatek will provide the following activities no later than 10 days prior to the contract end date.

- Provide an export of all regression and performance test artifacts, including but not limited to test scripts, test cases, test scenarios, etc.
- Provide a final copy of all software, compilation instructions and tools and final updated documentation.
- Provide an export of all issues and file attachments contained in the issue reporting system.
- Provide an export of all action items contained in the action item tracking tool.
- Provide an export of all finalized CR documents, including sample documents and templates used for the Change Request Process.
- Return all hardware and software that may be owned by the State upon request by the State. This includes system peripherals and other hardware.
- Maintain the collaboration web site to allow State staff (or designee) to download artifacts until the Contract expires or is terminated.
- Ensure appropriate development, test, business analyst and other Help Desk staff are retained until expiration or termination of the Contract.
- Provide technical training to the State (and/or its designee) for eighty (80) hours to include a thorough overview the system design, including a detailed walkthrough of the source code if requested, at a location to be determined by the State. Any unused Supplemental Service Hours may be utilized to provide additional training above these eighty (80) hours if requested by the State. These eighty (80) hours will not include Voyatek preparation time or travel time.
- Provide assurance and confirm that any data or system design provided by or for the State remains the property of the State and may not be marketed or sold by Voyatek without the express written consent of the State.
- Certify Voyatek compliance with State and Federal data retention requirements as stipulated in the Maintenance and Enhancement contract. At the request of the State, the Voyatek will destroy or purge any data provided by or for the State from all Voyatek database, electronic files, or paper files (including backups) at the end of any data retention period specified by the State. When completed, Voyatek will certify in writing that all data reference above has been destroyed or purged.

Voyatek will comply with all data security requirements of the Maintenance and Enhancement contract.

Appendix M: Partnerships and Contractual Relationships

Describe Vendor's partnerships and contractual relationships when Vendor uses subcontractor(s) to fulfill the requirements of this RFP. Describe the types of service(s), contractual relationship and the term of the contract between Vendor and its subcontractor(s).

The Partnerships and Contractual Relationships Plan below describes the process Voyatek would use if, during the North Carolina Crossroads Maintenance and Enhancement project, it becomes necessary to utilize one or more subcontractors to fulfill the requirements of the contract. As of March 6, 2025, Voyatek has not included any subcontractors as part of our proposal.

State of North Carolina

Department of Health and Human Services

Division of Child and Family Well-Being



Crossroads MIS

Maintenance and Enhancement Services

North Carolina WIC Program

Appendix M

Partnerships and Contractual Relationships

Trademarks

Trademarked names may appear throughout this document. Rather than list the names and entities that own the trademarks or insert a trademark symbol with each mention of the trademarked name, the names are used only for editorial purposes and to the benefit of the trademark owner with no intention of infringing upon that trademark.

Contact Information

To request copies, suggest changes, or submit corrections, contact:

North Carolina Department of Health and Human Services**Division of Child and Family Well-being, WIC Program**

Attention: Molly Jones

Crossroads WIC Release Manager

Phone: 252-903-3951

Email: Molly.Jones@dhhs.nc.gov

Revision History

Date	Version	Revised By	Description
12/18/2018	0.1	Jay Saunders, Three Sigma Software	Draft version
3/6/2025	1.0	Jennifer Saunders, Voyatek	Submission for RFP 30-25002-DCFW

Deliverable Description

This Partnerships and Contractual Relationships Plan describes the process Voyatek would use if during the North Carolina Crossroads Maintenance and Enhancement project is necessary to fulfill the requirements of the contract. As of 3/6/2025, Voyatek has not included any subcontractors as part of our proposal.

Contents

1. Partnership and Contractual Relationships	1

1. Partnership and Contractual Relationships

At the time of RFP Response, Voyatek does not expect to employ any subcontracts to fulfill the requirements of the RFP. In the event that Voyatek does engage a subcontractor to support the NC Crossroad, we will request written approval from North Carolina. The subcontract will be between Voyatek and the third-party vendor, and Voyatek will be responsible for all work provided by the subcontract vendor.

The Voyatek Product Manager is responsible for all work provided by subcontractors such that the employing entity, Voyatek or a subcontractor, will be transparent to North Carolina. As members of the Voyatek team, subcontractors will be assigned tasks and held accountable for completing tasks to the level of expectation that NC has come to expect from Voyatek. Subcontractors will provide status, complete necessary documentation, support team members, and communicate road-blocks and requests for assistance professionally and promptly. Subcontractors will be required to attend the appropriate Voyatek team meetings and project meetings based on their role on the project. Additionally, our risk assessment process includes review of subcontracts under the SOC 2 audit.

The Voyatek Contracts Department maintains the Voyatek Master Services Agreement (MSA) and related processes. The Contracts Department will work with the Voyatek Product Manager to define the scope of work to be performed by subcontract vendor. The MSA will identify pertinent timelines, expectations, and services to be rendered including adherence to all policies, plans, and schedules as approved for the North Carolina Crossroads Maintenance and Enhancement project.

Our MSA template includes such topics as listed below, but is not limited to the following:

- Relationship of parties
- Term of the agreement
- Termination for such events as:
 - o Default
 - o Client's Actions
 - o Non-availability of funding
 - o Voyatek Convenience
- Scope of work
- Payment and Invoicing
- Personnel provisions
 - o Substitution of personnel
 - o Work locations, including work will not be performed outside of the United States
- Confidentiality
- Work product and intellectual property
- Insurance
- Warranties

Appendix N: Help Desk Plan

The Help Plan below describes the approach to providing help desk services for the North Carolina Crossroads Maintenance and Enhancement project.

State of North Carolina

Department of Health and Human Services

Division of Child and Family Well-Being



Crossroads MIS

Maintenance and Enhancement Services

North Carolina WIC Program

Appendix N

Help Desk Plan

Trademarks

Trademarked names may appear throughout this document. Rather than list the names and entities that own the trademarks or insert a trademark symbol with each mention of the trademarked name, the names are used only for editorial purposes and to the benefit of the trademark owner with no intention of infringing upon that trademark.

Contact Information

To request copies, suggest changes, or submit corrections, contact:

North Carolina Department of Health and Human Services**Division of Child and Family Well-being, WIC Program**

Attention: Molly Jones

Crossroads WIC Release Manager

Phone: 252-903-3951

Email: Molly.Jones@dhhs.nc.gov

Revision History

Date	Version	Revised By	Description
12/18/2018	0.1	Jay Saunders, Three Sigma Software	Draft version
3/6/2025	1.0	Jennifer Saunders, Voyatek	Submission for RFP 30-25002-DCFW

Deliverable Description

This Help Plan describes the approach to providing help desk services for the North Carolina Crossroads Maintenance and Enhancement project.

Contents

1	Introduction	1
2	Voyatek’s Support Model.....	2
3	Helpdesk Solution Capabilities.....	4
4	Helpdesk Staff, Technical Support, Business Analyst Specialists Roles & Responsibilities	6
5	Helpdesk Processes and Procedures	7
5.1	General Help Desk Procedures	7
5.2	Specific Help Desk Procedures	7
5.2.1	Webinar/Shared Desktop Capabilities.....	7
5.2.2	Common library of debugging steps	7
5.2.3	Call Escalation	7
5.2.4	Help Desk Staff Training.....	7
5.3	Help Desk Staff access to technical and management staff	8
5.4	Help Desk Staff access to State environments	8
5.5	Tracking of Calls/Monitoring of volume	8
5.6	Identification of Common Issues/potential problems.....	8
5.7	Reporting Sample	8

Figures

Figure 1: Sample Open Tickets by Client by Age Report	9
Figure 2: Sample Tickets by Client, by Status report	9
Figure 3: Sample of Ring Central Agent Summary Dashboard	10
Figure 4: Ring Central Live Monitoring Dashboard	11

Tables

Table 1: Helpdesk Resources Roles and Responsibilities	6

1 Introduction

Voyatek will provide help desk support to assist with maintenance of the day-to-day operations of NC WIC and all its components including, portal, interfaces, batches, data, applications, reports and correspondences through an Incident and Problem Management process. Incident and Problem Management are the two primary activities of an application support organization. When executed in a holistic and industrialized manner, they serve to maximize application availability while minimizing the cost of application support.

Incident Management: The primary goal of Incident Management (IM) is to restore normal service operation as quickly as possible and minimize the adverse impact on business operations. Voyatek combines responsiveness based on application criticality with a cost-effective delivery model, resulting in a support structure that meets or exceeds business expectations at a predictable cost to serve.

Problem Management: Problem Management focuses on resolving the root cause of incidents, finding and implementing permanent solutions within the impacted application. Voyatek implements both reactive and proactive aspects of problem management. The reactive aspect is solving problems in response to one or more incidents. Proactive problem management is identifying and solving problems before incidents occur in production. We achieve this by leveraging reports of systemic issues across our client portfolio and implementing tight integration with the application development and infrastructure teams.

2 Voyatek's Support Model

Across our WIC customer base, Voyatek provides various levels of help desk support as required by each client. While we offer all levels of support, we have an appreciation for states that prefer to provide their own initial Help Desk support (often called Level 1) like NC WIC because the State team is always best equipped to provide guidance on specific State policies and procedures.

Voyatek will provide Help Desk support to the NC state office staff, when their initial help desk support is unable to resolve the issue, to help maintain the day-to-day operations of the NC WIC Crossroads MIS and all its components, interfaces, and data. We will do this utilizing our team of NC Crossroads subject matter and technical experts, all of whom are in the continental United States. This team is the same team that NC WIC has come to know and trust over the past six years. Our team's ability to understand and diagnose problems quickly and efficiently to ensure minimal disruption to the NC clinic and state staff is a significant part of the value proposition that Voyatek offers to North Carolina.

During Transition-In, we will confirm the direct contact information for our NC Crossroads subject matter and technical experts so that NC WIC has the most efficient support for the state office staff. In addition, we will provide a dedicated toll-free phone number for our traditional Help Desk so that if our dedicated NC Crossroads team is unavailable, the NC WIC staff can contact our Help Desk to receive prompt support for reported issues during normal business hours. Our Help Desk team will record reported issues in their issue management system and will contact our NC Crossroads support team to initiate a timely and efficient response.

By providing these two methods of reaching our NC Crossroads team, we ensure that the NC WIC team will always have their calls answered. In addition to phone calls, for lower priority issues, the NC WIC staff may opt to send emails directly to our team. The NC Crossroads product team has a demonstrated track record of being responsive and efficient in tracking and resolving issues for NC WIC. They have the knowledge and capability to handle a minimum of 25 issues per quarter as required by the RFP.

The Voyatek teams use Azure DevOps to organize and manage most aspects of our technical support, and this includes logging of all help desk tickets for the NC Crossroads product team to address. We will continue to provide access to Azure DevOps for the NC WIC state office staff to allow them to view, update, and add defect information directly into Azure DevOps. All issues that were initiated by a phone call or email will be logged into DevOps by the Voyatek team. Tickets needing immediate attention are marked as urgent and escalated to a Voyatek team member.

The support model consists of the following levels:

Level 1: Voyatek Help Desk is the backup point of contact for state users if the Voyatek dedicated NC Crossroads team is unavailable. The Voyatek Help Desk will capture incident details, which is used for issue tracking, priority, and severity. Based on the nature of the incident of the call, our help desk staff will immediately route the caller to the appropriate Voyatek NC Crossroads staff. The NC Crossroads staff will work with the caller to resolve this issue.

Level 2: Voyatek’s NC Crossroads Technical Support and Business Analyst Specialists provide the core of the Level 2 support service. The Technical Support and Business Analyst Specialists resources will have specific knowledge of the NC WIC Crossroads and the business processes they support. They will be involved in modifications to application configurations, correction or extraction of data and implementation of a work around to a problem that requires modifications to application code.

Level 3: For incidents that require code modifications or detailed technical knowledge of the applications, our Level 3 resources are engaged. This team resolves complex production issues escalated from Level 2 or spawned by our application monitoring. This team is responsible for updating knowledge base artifacts and driving higher resolution rates within the Service Desk. The Level 3 team will be responsible for resolving system processes and troubleshooting issues for NC Crossroads through application monitoring. Application monitoring will focus on resolution of outages, hung processes, data issues, or other issues that negatively impact the application cycle.

3 Helpdesk Solution Capabilities

Voyatek's traditional Help Desk Solution is configured to capture reported issues electronically through e-mail or via a standard call number (these will be provided to NC during Transition-In). Once an issue is reported, it is prioritized and routed to the appropriate support level for resolution and reported to the users and management.

Voyatek Help Desk staff will:

- Answer calls and emails
- Record service requests
- Track and monitor requests for IT services
- Resolve common technical support issues
- Triage unsolved new MIS Help Desk issues
- Ensure the Known Error Database (KEDB) is kept current regarding known errors and their resolutions.
- Develop and maintain Frequently Asked Questions (FAQs) and self-help guidance documents that the State will publish in the new MIS and/or on the WIC website

The Help Desk ticketing system will capture the following information:

- Time and date of call
- First and last name of caller
- Clinic name/location
- Computer type, Crossroads system module (clinic, vendor, etc.) and operating system
- Call category (e.g., equipment, WIC Program, new MIS or EBT for WIC application)
- Call priority level
- Type of problem reported
- Detailed description of problem
- Detailed description of solution
- Audit trail (call status)
- Call resolution

The Help Desk will maintain and report on the following call center service performance metrics:

- Number and percent of calls resolved
- Average hold or waiting time

- Abandoned call rate or percent of abandoned calls
- Number of calls by priority level
- Backlog of open or pending tickets
- Ticket distribution by functional area

4 Helpdesk Staff, Technical Support, Business Analyst Specialists Roles & Responsibilities

Table 1: Helpdesk Resources Roles and Responsibilities

Team	Role	Responsibilities
Voyatek	Help Desk Manager	• Manage day-to-day activities of the Help Desk, including staffing, interviewing, hiring, performance management, and quality assurance and performance improvement. • Manage day to day staffing plans and operations. • Provide training and quality control. • Organize and oversee staff development. • Ensure that staff meets SLAs as identified by the State. • Facilitate the escalation process. • Analyze call volume trends to anticipate staffing needs. • Provide reporting metrics for analysis.
Voyatek	Help Desk Staff	• Receive phone calls or emails from North Carolina staff and provide support per the training and information provided. • Open tickets and save data to knowledge database as required • Provide accurate and clear descriptions in tickets and according to the Escalation Grid ensure that tickets are escalated properly, and the appropriate Voyatek Crossroads Technical Support and Business Analyst Specialists are connected with the customer
Voyatek	Technical Support and Business Analyst Specialists	• Receive phone calls/emails from North Carolina state staff and provide support per request. • Apply Crossroads knowledge and experience to resolve issue for customer. • When appropriate, make entries into Azure DevOps system to identify potential problem areas.

5 Helpdesk Processes and Procedures

5.1 General Help Desk Procedures

The most important part of handling any issue or request through the help desk is to ensure that adequate information is gathered at the start of the call to fully understand the issue that is being presented or the request that is being made of the help desk. This requires a list of questions designed to effectively gather that information efficiently. This troubleshooting checklist will ensure that if an issue needs to be escalated for resolution, the next resource working on the issue or request can do so without contacting the user again. This checklist will reside within the knowledge base to be referenced on each call. The knowledge base will be a key repository of all documented processes and procedures for the help desk. This will include step by step walk through to include screen shots and escalation procedures.

The Voyatek Help Desk team will be using the existing Ring Central phone system and ConnectWise ticketing system currently in place at the Voyatek development facility. The Voyatek Help Desk team will configure the Ring Central virtual call center to accommodate the addition of the North Carolina customer who needs specific Crossroads assistance. The Voyatek team will report on trends and corresponding actions that will determine if the problems surround technical issues, application issues, training, or lack of, as well as communications that can resolve the issues.

5.2 Specific Help Desk Procedures

5.2.1 Webinar/Shared Desktop Capabilities

Voyatek staff will make use of the existing MS Teams teleconference system to allow for the sharing of desktops to assist with troubleshooting. Callers can be invited to connect to a teleconference to share their desktop screens. This will allow Voyatek personnel to more quickly pinpoint issues and potential problems.

5.2.2 Common library of debugging steps

Voyatek staff will make use of the existing ConnectWise to allow for maintenance of a common library of issues and resolution steps. If a new problem arises requiring a new release, the Technical Support staff will assist with workaround solutions until a release can be scheduled and implemented.

5.2.3 Call Escalation

Voyatek staff will escalate calls as described above. By making use of and monitoring the ticketing system, Voyatek staff will be aware of North Carolina reports of issues that may be affecting multiple clinics or perhaps a system wide issue. These will be reported immediately to the State office while the team works on resolving the issue.

5.2.4 Help Desk Staff Training

Voyatek has internal procedures that leverage the training material we provide to our customers to train any new staff that may need to be hired. Additionally, we hold bi-weekly companywide WIC regulation training and awareness sessions. This way, any new regulations or system changes are quickly promulgated to the entire staff.

5.3 Help Desk Staff access to technical and management staff

The Help Desk staff have immediate access to both technical and management staff. For example, if a phone line is busy and an urgent situation has arisen, help desk staff will utilize MS Teams to send an urgent message to the Technical, Business Analyst or Management staff.

5.4 Help Desk Staff access to State environments

Help desk staff will be part of the overall Voyatek Crossroads support team and will request access through the Product Manager to the State as appropriate. This will allow for real-time resolution of issues.

5.5 Tracking of Calls/Monitoring of volume

Voyatek Help Desk staff will use its existing Ring Central call system, and existing ConnectWise ticketing system to track and monitor calls and emails to the help desk.

5.6 Identification of Common Issues/potential problems

By having immediate access to the ConnectWise ticketing system, the Help Desk staff will be able to see patterns of potential emerging problems. Dashboards and reporting capabilities of the ConnectWise will allow for analysis of issues and identification of potential problems.

5.7 Reporting Sample

The ConnectWise system contains many built-in reporting features and is also supported by an SQL database, so if needed, custom reports can be built accessing any needed data element. An example of one of the built-in reports, with various filters/sorting orders, is shown below.

Open Tickets by Client by Age

Company Name

Ticket#	Age	Summary Description	Hours Worked	Contact	Status	Team	Entered
57715	1	Managed Services	0	Gail Thompson	Waiting on Sales	Sales Team	04/30/2014 8:46am
57357	1	printer help :(	2	Rebekah Clark	Waiting on Parts	Service Team	04/28/2014 1:41pm
56553	8	Reopen Ticket: # 54817 regarding Computer Prob	0.5	Rebekah Clark	Closed	Service Team	04/22/2014 9:20am
56506	9	NEW EMPLOYEES LIST, setup on network	1.5	Gail Thompson	Waiting on custor	Service Team	04/21/2014 3:02pm

Figure 1: Sample Open Tickets by Client by Age Report

Tickets by Client, by Status

Company Name

Start Date

End Date

Ticket#	Entered	Age	Summary Description	Contact	Status	Team
15118	03/13/2013	8	5.1 FW: VMware Support and Subscription Confirmation - Ord	James Truax	>Completed	Orders board
Total Tickets: Completed Status 1						
59062	05/12/2014	8	0.1 Certificate alert in Outlook	James Truax	>New	Internal Network Team
Total Tickets: New Status 1						
59147	05/12/2014	1	0 MS SQL Server Reporting for LOGAN-VCENTER at Roeing\Lc	James Truax	>Resolved	Managed Services Tea
59143	05/12/2014	1	0 MS SQL Server Reporting for LAF-COMM at Roeing\Lafayet	James Truax	>Resolved	Managed Services Tea
59139	05/12/2014	1	0 MS SQL Server Reporting for LAF-VCENTER at Roeing\Lafay	James Truax	>Resolved	Managed Services Tea
59134	05/12/2014	1	0 MS SQL Server Reporting for LAF-NAS at Roeing\Lafayette	James Truax	>Resolved	Managed Services Tea
59132	05/12/2014	1	0 MS SQL Server Reporting for LOGAN2K3-BDC at Roeing\Lo	James Truax	>Resolved	Managed Services Tea
59126	05/12/2014	1	0 MS SQL Server Reporting for LAF-DEV-12APP2 at Roeing\La	James Truax	>Resolved	Managed Services Tea
59121	05/12/2014	1	0 MS SQL Server Reporting for LAF-BACKUP at Roeing\Lafaye	James Truax	>Resolved	Managed Services Tea
59112	05/12/2014	1	0 MS SQL Server Reporting for LAF-SQL3 at Roeing\Lafayette	James Truax	>Resolved	Managed Services Tea
59105	05/12/2014	1	0 MS SQL Server Reporting for LOGAN-FS2 at Roeing\Logan	James Truax	>Resolved	Managed Services Tea
59104	05/12/2014	1	0 MS SQL Server Reporting for LAF-SQL at Roeing\Lafayette	James Truax	>Resolved	Managed Services Tea
59093	05/12/2014	1	0.1 Exchange Server Email Stats for LAF-EX2010	James Truax	>Resolved	Managed Services Tea
59087	05/12/2014	1	0.1 Exchange Server Email Stats for LAF-EX2010	James Truax	>Resolved	Managed Services Tea
59059	05/12/2014	6	0.2 Change Control - Server Role Detection Roeing\LAF-SQL	James Truax	>Resolved	Managed Services Tea
59045	05/11/2014	1	0.6 SVC - Auto Services Stopped:8 - LAF-14-LYNC1 1001 wua	James Truax	>Resolved	Managed Services Tea
59043	05/11/2014	7	0.7 Perf - OWA Average Response Time:457441 - LAF-EX2010	James Truax	>Resolved	Managed Services Tea
Total Tickets: Resolved 15						
Grand Total # Tickets 17						

Figure 2: Sample Tickets by Client, by Status report

In addition, we can track call volume via our Ring Central system. An example of a Ring Central Agent Summary screen is shown below.

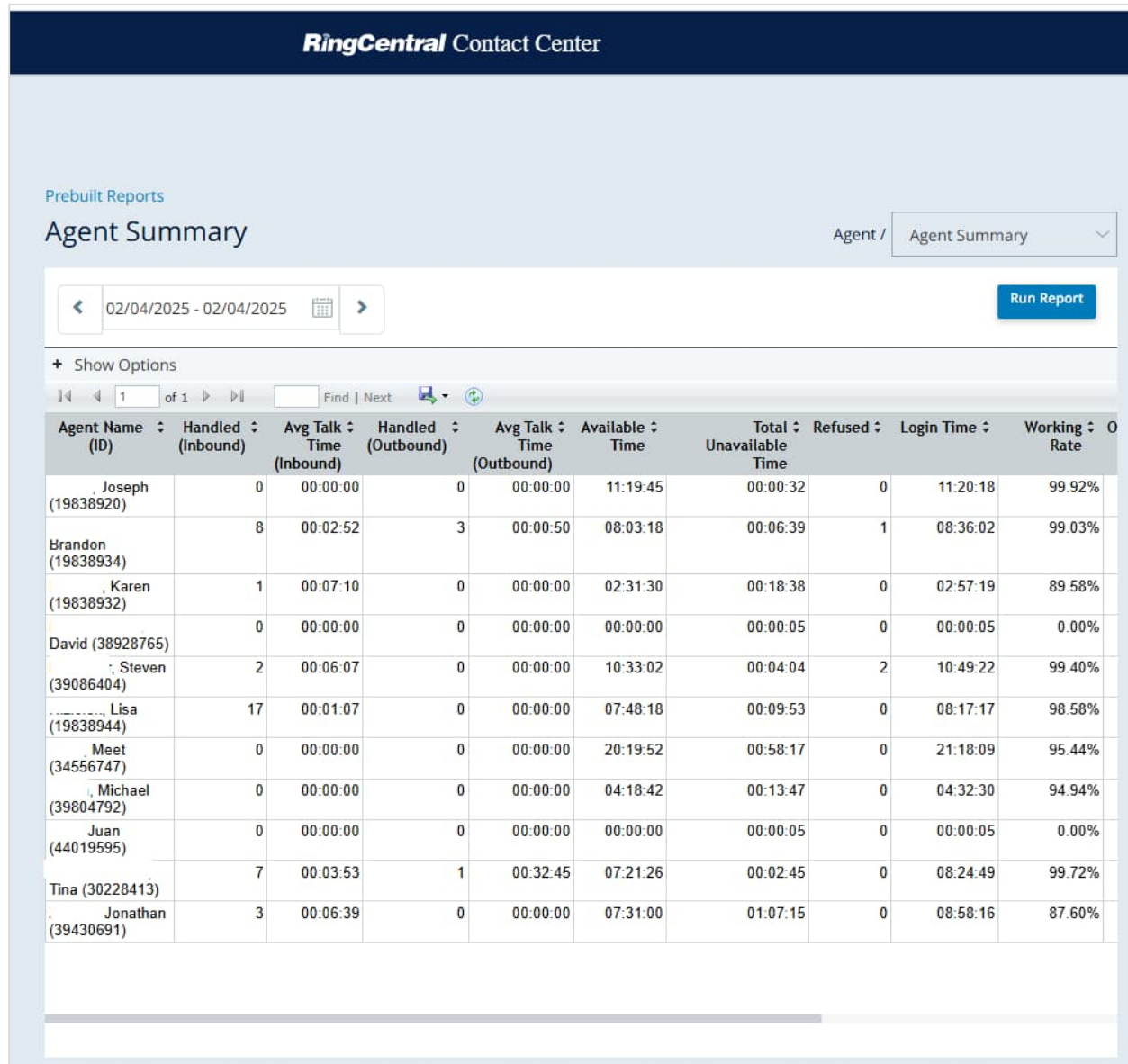


Figure 3: Sample of Ring Central Agent Summary Dashboard

An Example of Live call monitoring.

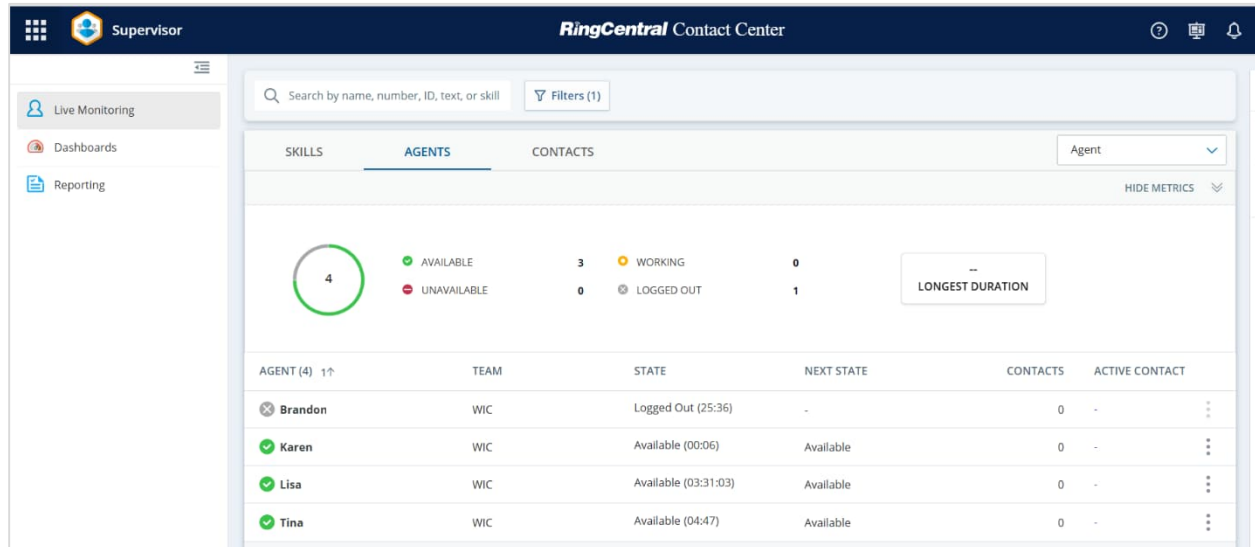


Figure 4: Ring Central Live Monitoring Dashboard

Staff performance

Voyatek help desk staff will be configured so that calls will be answered by live staff within one minute. By integrating our Crossroads staff with our existing help desk capability, North Carolina can leverage the existing help desk at minimal cost.

If the helpdesk staff are notified by the State of a critical statewide production down issue, Voyatek will provide written acknowledgement to the reporting State staff and the Crossroads WIC MIS Release Manager within fifteen minutes confirming that appropriate staff are working the issue.

Appendix P: Communication and Coordination Plan

The Communication and Coordination Plan outlined below delineates the detailed communication strategy for the project. This includes various activities such as status reports, conference calls, and on-site visits. The Plan encompasses all stakeholders involved in the project, including state representatives, state contracted IV&V staff, the WIC EBT Contractor, local WIC agencies/clinics, the prime contractor, and other significant parties. It provides a detailed framework for how communications among and between stakeholders will be executed and managed effectively.



Crossroads MIS
Maintenance and Enhancement Services

North Carolina WIC Program

Appendix P
Communication and Coordination Plan

Trademarks

Trademarked names may appear throughout this document. Rather than list the names and entities that own the trademarks or insert a trademark symbol with each mention of the trademarked name, the names are used only for editorial purposes and to the benefit of the trademark owner with no intention of infringing upon that trademark.

Contact Information

To request copies, suggest changes, or submit corrections, contact:

North Carolina Department of Health and Human Services**Division of Child and Family Well-being, WIC Program**

Attention: Molly Jones

Crossroads WIC Release Manager

Phone: 252-903-3951

Email: Molly.Jones@dhhs.nc.gov

Revision History

Date	Version	Revised By	Description
12/18/2018	0.1	Jay Saunders, Three Sigma Software	Draft version
3/6/2025	1.0	Jennifer Saunders, Voyatek	Submission for RFP 30-25002-DCFW

Deliverable Description

The Communication and Coordination Plan will describe the communication approach, including events such as status reports, conference calls, on-site visits, etc. The Plan should include all stakeholders involved in the project, including the State, State contracted IV&V staff, the WIC EBT Contractor, the local WIC agencies/clinics, the prime, and other major related parties. The Communication and Coordination Plan should detail how communications among and between stakeholders will be delivered and managed.

Contents

1. Introduction	1
2. Communications Management Approach	2
3. Communications Management Constraints	3
4. Stakeholder Communication Requirements.....	4
5. Roles	5
6. Project Team Directory.....	7
7. Communication Methods and Technologies	8
8. Communication Matrix	9
9. Communication Flowchart.....	13
10. Guidelines for Meetings	14
11. Guidelines for Monthly Project Status Reports.....	15
12. Communication Standards	16
13. Communication Escalation Process	17
14. Glossary of Communication Terminology	18

Figures

Figure 1: Communication Flowchart	13

Tables

Table 1: Communication and Coordination Plan Contact Information	7
Table 2: Communication Requirements Matrix	9
Table 3: Communication Escalation Process.....	17
Table 4: Glossary of Communication Terminology	18

1. Introduction

The purpose of the Communication and Coordination Plan is to define the communication requirements for the project and how information will be distributed. The Communication and Coordination Plan defines the following:

- What information will be communicated—to include the level of detail and format
- How the information will be communicated—in meetings, email, telephone, web portal, etc.
- When information will be distributed—the frequency of project communications both formal and informal
- Who is responsible for communicating project information
- Communication requirements for all project stakeholders
- What resources the project allocates for communication
- How changes in communication or the communication process are managed
- The flow of project communications
- Any constraints, internal or external, which affect project communications
- Any standard templates, formats, or documents the project must use for communicating
- An escalation process for resolving any communication-based conflicts or issues

This Communication and Coordination Plan sets the communications framework for this project. It will serve as a guide for communications throughout the life of the project and will be updated as communication needs change. This plan identifies and defines the roles of persons involved in this project. It also includes a communications matrix that maps the communication requirements of this project. An in-depth guide for conducting meetings details both the communications rules and how the meetings will be conducted, ensuring successful meetings. A project team directory is included to provide contact information for all stakeholders directly involved in the project.

2. Communications Management Approach

Approximately 80% of a project manager's time is spent communicating.

The Voyatek Product Manager will take a proactive role in ensuring effective communications on this project. The communications requirements are documented in the Communications Matrix presented in this document. The Communications Matrix will be used as the guide for what information to communicate, who is to do the communicating, when to communicate it and to whom to communicate.

As with most project plans, updates or changes may be required as the project progresses or changes are approved. Changes or updates may be required due to changes in personnel, scope, budget, or other reasons. Additionally, updates may be required as the project matures and additional requirements are needed. The Voyatek Product Manager is responsible for managing all proposed and approved changes to the Communication and Coordination Plan. Once the change is approved, the Product Manager will update the plan and supporting documentation and will distribute the updates to the project team and all stakeholders to so that all project stakeholders remain aware and informed of any changes to communications management.

3. Communications Management Constraints

All project communication activities will occur within the project's approved budget, schedule, and resource allocations. The Voyatek Product Manager is responsible for ensuring that the project team performs communication activities. Communication activities will occur in accordance with the frequencies detailed in the Communication Matrix so that the project adheres to schedule constraints. Any deviation of these timelines may result in schedule delays and must be approved by the Crossroads WIC MIS Release Manager.

The Voyatek Product Manager is responsible for ensuring that approval is requested and obtained prior to the distribution of any sensitive information regarding this project.

4. Stakeholder Communication Requirements

As part of identifying all project stakeholders, the Voyatek Product Manager will coordinate with the Crossroads WIC Release Manager to determine the preferred frequency and method of communication with each stakeholder. Standard project communications will occur in accordance with the Communication Matrix; however, all communications to the North Carolina Department of Health and Human Services will be coordinated through the Crossroads WIC Release Manager.

In addition to identifying communication preferences, stakeholder communication requirements must identify the project's communication channels and so that stakeholders have access to these channels. If project information is communicated via secure means or through internal company resources, all stakeholders, internal and external, must have the necessary access to receive project communications.

Once all stakeholders have been identified and communication requirements are established, the project team will maintain this information in the project's Stakeholder Register and use this, along with the project communication matrix as the basis for all communications. The Stakeholder Register will be posted to the Project SharePoint site.

5. Roles

DPH/DHHS Management/Project Sponsor

The DPH WIC office is the champion of the project and has authorized the project within DHHS. The Project Sponsor within DPH WIC is responsible for the funding of the project and is ultimately responsible for its success. Because the Project Sponsor is at the executive level, communications should be presented in summary format unless the Project Sponsor requests more detailed communications.

Crossroads WIC Release Manager

The Crossroads WIC Release Manager will be the primary point through which all communications to and from DHHS/WIC will be channeled. The Crossroads WIC Release Manager will, in turn, distribute information and documents within the NC WIC Program stakeholder groups as appropriate. The Crossroads WIC Release Manager will be accepting the final deliverables of this project and will be kept informed of the project status, including potential impacts to the schedule for the final deliverables or the product itself.

Voyatek Product Manager

The Product Manager has overall responsibility for the execution of the project. The Product Manager manages day to day resources, provides project guidance and monitors and reports on the projects metrics as defined in the Project Management Plan. As the person responsible for the execution of the project, the Product Manager is the primary communicator for the project distributing information according to this Communication and Coordination Plan.

Similarly to how the Crossroads WIC Release Manager is the primary point through which all communications to and from DHHS/WIC will be channeled, the Voyatek Product Manager is the primary point through which all communications to and from Voyatek staff will be channeled. The Voyatek Product Manager will issue any program direction and guidance.

Business Analyst Manager

The Business Analyst Manager will manage the Voyatek team's business analysis activities, to include requirements specification, functional design, and gap analysis for new features. This includes the work required to identify, manage, and document the impacts, cost, benefits, issues, and consequences resulting from any changes in scope, requirements, design, plans, or work assignments. The Business Analyst Manager will facilitate working sessions to understand, analyze, and derive WIC processes, business rules, and data relationships. The Business Analyst Manager will also be the initial contact for help desk requests and will coordinate research and testing of reported issues with other team members.

Development Manager

The Development Manager is responsible for ensuring that all technical aspects of the project are addressed and that the project is implemented in a technically sound manner. The Development Manager is responsible for all technical designs, overseeing the implementation of the designs and developing/maintaining as-build documentation. The Development Manager requires close communications with the Product Manager and the Project Team. The Development Manager will

provide guidance and direction to Voyatek's development team so that design, development, and configuration activities follow applicable standards, and that system objects and documentation are consistent across developers.

Test Manager

The Test Manager is responsible for developing, managing, and coordinating all test activities for each System release. The Test Manager will assist the Development Manager and Business Analyst Manager to update documents to appropriately reflect changes to the system throughout the maintenance and enhancement process. The Test Manager will oversee the Voyatek team to develop the Test Plans, Test Cases, Test Scripts, Test Procedures, Test Data, and Test Results Reports for each test phase for each System release. The Test Manager will also manage the test environment such that the environment for each test phase and System release is prepared on schedule. The Test Manager will also validate software and work product/ documentation quality for each release.

Voyatek Project Team

The Project Team is comprised of all persons who have a role performing work on the project. The project team needs to have a clear understanding of the work to be completed and the framework in which the project is to be executed. Because the Project Team is responsible for completing the work for the project, they played a key role in creating the Project Plan including defining its schedule and work packages. The Project Team requires a detailed level of communications which is achieved through day to day interactions with the Voyatek Product Manager and other team members along with weekly team meetings.

6. Project Team Directory

The following table presents contact information for all persons identified in this Communication and Coordination Plan including their email addresses and phone. Phone numbers will be confirmed during Transition In.

Table 1: Communication and Coordination Plan Contact Information

Role/Title	Name	Organization/ Department	Email
DHHS/WIC Project Sponsor	TBD	DHHS State WIC Director	TBD
Crossroads WIC Release Manager	Molly Jones	NC DHHS	Molly.Jones@dhhs.nc.gov
Voyatek Product Manager	Jennifer Saunders, PMP	Voyatek	Jennifer.saunders@voyatek.com
Business Analyst Manager	Cindy Kochersperger	Voyatek	Cindy.Kochersperger@voyatek.com
Test Manager	Helena Young	Voyatek	Helena.Young@voyatek.com
Development Manager	Michael Heinrich	Voyatek	Michael.Heinrich@voyatek.com

7. Communication Methods and Technologies

Voyatek maintains a SharePoint site for all projects, which will be used to provide updates, archive various reports, and conduct project communications. This platform enables senior management, as well as stakeholders to access project data and communications at any point in time. SharePoint also provides the ability for stakeholders and project team members to collaborate on project work and communication.

Voyatek maintains software licenses for MS Project software. All project teams are responsible for developing, maintaining, and communicating schedules using this software. GANTT Charts are the preferred format for communicating schedules to stakeholders. The project schedule will be maintained on the SharePoint site.

All project communication and documentation will be maintained on the SharePoint platform. Standardized naming conventions for files and folders will be applied to all documents.

Voyatek will utilize MS Teams for teleconferencing and chat. This platform will allow State personnel and 3rd party Vendors to participate in meetings. North Carolina and Voyatek are able to use MS Teams Chat features without scheduling meetings. This has proven helpful when coordinating schedules and needing to communicate quickly.

8. Communication Matrix

The following table identifies the communications requirements for this project.

Table 2: Communication Requirements Matrix

What	Who/Target	Purpose	When/Frequency	Type/Method(s)
Voyatek Team Initiation Meeting	Voyatek Staff	Gather information for Initiation Plan	One time	Meeting
Distribute Project Initiation Plan	Voyatek Staff	Provide consistent guidance for the team to continue their support to NC WIC	One time	Document distributed via email
Project Kick Off with NC WIC	All stakeholders	Communicate plans and stakeholder roles/responsibilities Encourage communication among stakeholders.	TBD, within 4 weeks of project start – One time meeting	Meeting at NC WIC office or location mutually agreed upon with NC WIC or MS Teams meeting. Voyatek Product Manager will distribute meeting notes via email and or posting on SharePoint site
Weekly Status Meetings	All stakeholders	Update stakeholders on progress of the project	Regularly Scheduled: Weekly	MS Teams meeting hosted by Voyatek. Crossroads WIC MIS Release Manager maintains and distributes the agenda via email. Distribute via email or by posting on SharePoint site
Monthly Status Reports	Crossroads WIC MIS Release Manager	Update stakeholders on progress of the project	Regularly Scheduled: Monthly	Voyatek emails to Crossroads WIC MIS Release Manager. Distribute via email

What	Who/Target	Purpose	When/Frequency	Type/Method(s)
Monthly Managed Services Report	Crossroads WIC MIS Release Manager	Update NC WIC on the hosting and maintenance services for Crossroads	Regularly scheduled: Monthly	Voyatek emails to Crossroads WIC MIS Release Manager. Distribute via email within the Monthly Status Report
Quarterly Project Meetings	All stakeholders	Update stakeholders on progress of the project	Regularly Scheduled: Quarterly	At least one quarterly meeting must be on-site at NC WIC offices, or other location as appropriate. Otherwise, MS Teams meeting hosted by NC WIC.
Topic Call	NC-Voyatek Team	To plan in-progress and upcoming activities, review tasks, timelines and answer questions	Regularly Scheduled: Weekly	MS Teams meeting hosted by NC WIC. Crossroads WIC MIS Release Manager maintains and distributes the agenda via email. Distribute via email and or by posting on SharePoint site
Team Meetings	Voyatek Project Team. Individual meetings for sub-teams, technical team, and Functional teams as appropriate.	To review detailed plans (tasks, assignments, and action items)	Regularly Scheduled: Mondays, Wednesdays, Thursdays, and as needed	MS Teams Meeting hosted by Voyatek

What	Who/Target	Purpose	When/Frequency	Type/Method(s)
Special Projects	Voyatek Project Team	To review detailed plans specific to special projects (e.g., Telehealth portal)	Regularly Scheduled based on project	MS Team meeting hosted by Voyatek
Joint Application Development (JAD) Sessions	Specific individuals from the NC WIC and Voyatek staff best suited for the particular JAD topic.	To rapidly and jointly development application requirements and capabilities.	As required during the enhancement development cycle	MS Team meeting/Report
Post Project Review	Voyatek Product Manager, Crossroads WIC MIS Release Manager	Identify improvement plans, lessons learned, what worked and what could have gone better. Review accomplishments.	End of significant enhancements or projects.	MS Team Meeting/Report
Presentations to Special Interest Groups	Examples: Local Agency Staff	To update external groups to promote communication and create awareness of project interdependencies.	At project milestones so as to communicate with other interested parties of changes that will be introduced outside of the Project Team.	Presentation/Demonstration in format appropriate to the situation

What	Who/Target	Purpose	When/Frequency	Type/Method(s)
SharePoint Site	Designated Project Members.	Central location to house Status Reports, meeting minutes, Project description, and Project Plans.	Update monthly with Status Reports; otherwise, as necessary.	Electronic Communications Venue. Lists and folders for tracking action items and document sharing
Periodic Demos and Target Presentations	Specific Groups or End Users. Examples: Local Agency and Clinic personnel.	To gain input from special groups and keep them abreast of the Project's status.	As team completes critical phases or makes major enhancements.	Presentation/Discussion
Informal and other unscheduled meetings or announcements	To be determined by the Project Team	General communications	As needed	Lunch and Learn sessions, email lists, SharePoint announcements, etc.

9. Communication Flowchart

The communication flowchart below was created to aid in project communication. This flowchart provides a framework for the project team to follow for this project. However, there may be occasions or situations which fall outside of the communication flowchart where additional clarification is necessary. In these situations, the Product Manager is responsible for discussing the communication with the Project Sponsor and making a determination on how to proceed.

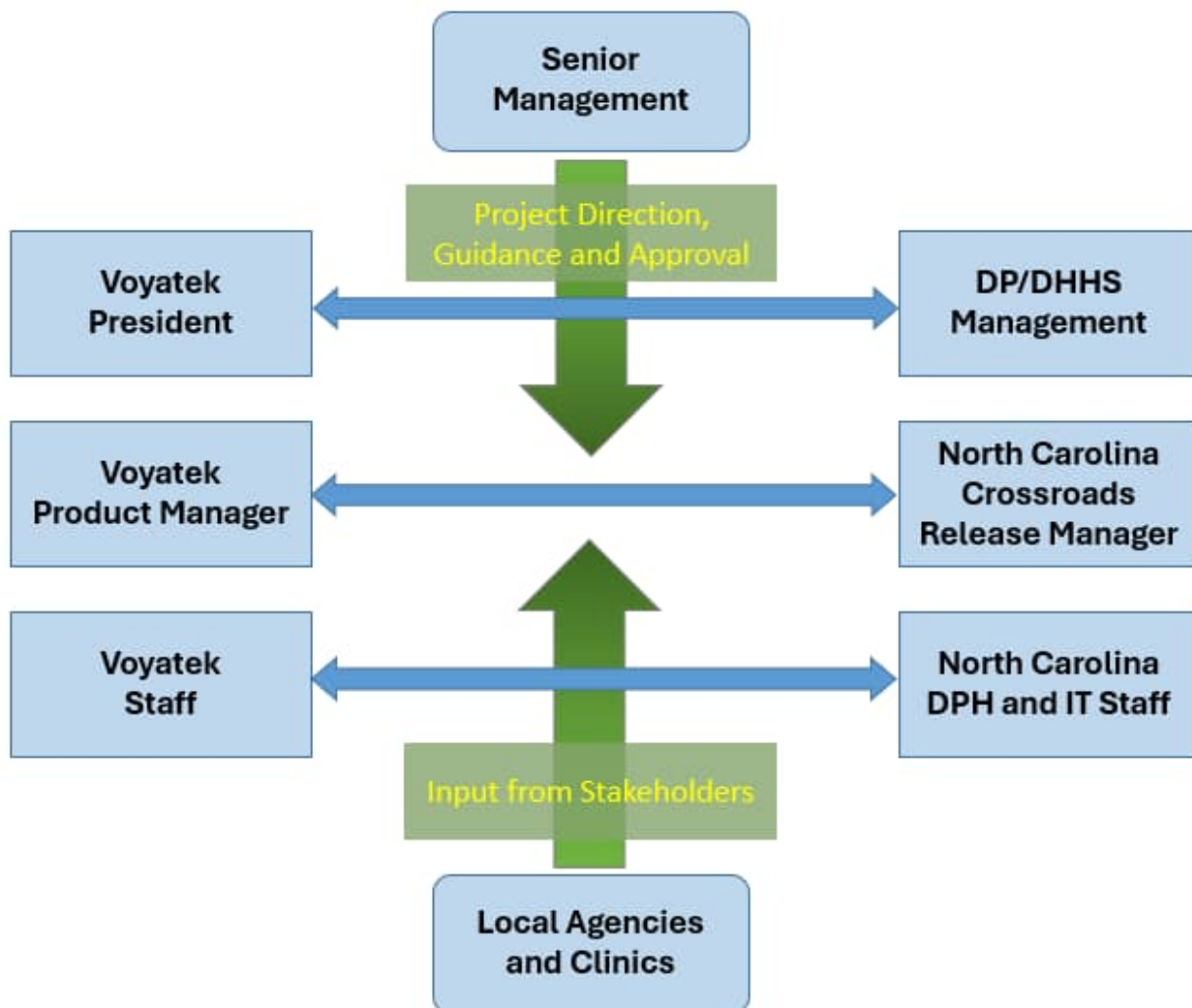


Figure 1: Communication Flowchart

10. Guidelines for Meetings

Meeting Agenda

Meeting Agenda will be distributed 5 business days in advance of the meeting. The Agenda will identify the presenter for each topic along with a time limit for that topic. The first item in the agenda will be a review of action items from the previous meeting.

Meeting Minutes

Meeting minutes will be distributed within 2 business days following the meeting. Meeting minutes will include the status of all items from the agenda along with new action items and the Parking Lot list.

Action Items

Action Items are recorded in both the meeting agenda and minutes. Action items are also tracked with SharePoint lists for ease of access by both Vendor and State personnel. Action items will include both the action item along with the owner of the action item. Meetings will start with a review of the status of all action items from previous meetings and end with a review of all new action items resulting from the meeting. The review of the new action items will include identifying the owner for each action item.

Meeting Chairperson

The Chairperson is responsible for distributing the meeting agenda, facilitating the meeting and distributing the meeting minutes. The Chairperson will ensure that the meeting starts and ends on time and that all presenters adhere to their allocated time frames.

Note Taker

The Note Taker is responsible for documenting the status of all meeting items, maintaining a Parking Lot item list and taking notes of anything else of importance during the meeting. The Note Taker will give a copy of their notes to the Chairperson at the end of the meeting as the Chairperson will use the notes to create the Meeting Minutes.

Timekeeper

The Timekeeper is responsible for helping the facilitator adhere to the time limits set in the meeting agenda. The Timekeeper will let the presenter know when they are approaching the end of their allocated time. Typically, a quick hand signal to the presenter indicating how many minutes remain for the topic is sufficient.

Parking Lot

The Parking Lot is a tool used by the facilitator to record and defer items which are not on the meeting agenda; but merit further discussion at a later time or through another forum.

A parking lot record should identify an owner for the item as that person will be responsible for ensuring follow-up. The Parking Lot list is to be included in the meeting minutes.

11. Guidelines for Monthly Project Status Reports

Voyatek will provide thorough monthly project status reports in a format that is agreeable to the State. A discussion of the specific content of project status reports will be conducted with the State at project initiation; the team will develop a status report format that will be used throughout the project. The status report will also be used to track progress against the Work Plan. Voyatek typically includes the following information in our standard status report format; however, we will tailor the report to the State's needs.

General Information. Identifies project name, reporting period, and staff completing the report.

Project Status Summary: Provides a summary of activities that have occurred during the reporting period. Including:

- Work accomplished in the reporting period;
- Production Issues
- Release In Progress Status
- Risk Tracking Log
- Service Level Agreement
- Managed Services/Hosting Status
- Change Requests
- Special Project Status

Project Schedule/ WBS Updates

Updates to the Project Schedule and WBS will be documented in the Status Report as applicable.

Detailed Issues Log

Details any issues that have been identified throughout the course of the project. Each issue will be logged with a description of the problem, given an issue number and assigned to an individual or entity. The log will include the suggested mitigation/resolution strategy and a timeframe for resolution. Once resolved, the actual resolution will be documented along with the date of the resolution.

12. Communication Standards

For this project, Voyatek will utilize standard organizational formats and templates for all formal project communications. Formal project communications are detailed in the project's communication matrix and include:

- 1) Kickoff Meeting
- 2) Project Team Meetings
- 3) Technical Design Meetings
- 4) Weekly Project Status Meetings
- 5) Monthly Project Status Reports

Informal project communications should be professional and effective but there is no standard template or format that must be used.

13. Communication Escalation Process

Efficient and timely communication is the key to successful project completion. As such, it is imperative that any disputes, conflicts, or discrepancies regarding project communications are resolved in a way that is conducive to maintaining the project schedule, ensuring the correct communications are distributed, and preventing any ongoing difficulties. To maintain the project schedule and resolve issues in a timely manner, Voyatek will use a standard escalation model to provide a framework for escalating communication issues. The table below defines the priority levels, decision authorities, and timeframes for resolution.

Table 3: Communication Escalation Process

Priority	Definition	Decision Authority	Timeframe for Resolution
Priority 1	Major impact to project or business operations. If not resolved quickly there will be a significant adverse impact to schedule.	Voyatek President	Within 4 hours
Priority 2	Medium impact to project or business operations which may result in some adverse impact to schedule.	Product Manager	Within one business day
Priority 3	Slight impact which may cause some minor scheduling difficulties with the project	Product Manager	Within two business days
Priority 4	Insignificant impact to project but there may be a better solution.	Product Manager	Work continues and any recommendations are submitted via the project change control process

14. Glossary of Communication Terminology

Table 4: Glossary of Communication Terminology

Term	Definition
Communication	The effective sending and receiving of information. Ideally, the information received should match the information sent. It is the responsibility of the sender to ensure this takes place.
Stakeholder	Individuals or groups involved in the project or whose interests may be affected by the project's execution or outcome.
Communication and Coordination Plan	Portion of the overall Project Management Plan which details how project communications will be conducted, who will participate in communications, frequency of communications, and methods of communications.
Escalation	The process which details how conflicts and issues will be passed up the management chain for resolution as well as the timeframe to achieve resolution.

Appendix Q: SOC 2

The following pages represent the System and Organization Controls 2 (SOC 2) report for the period of March 1, 2023 – February 29, 2024.

REDACTED

Appendix R: Optional Services

Voyatek has provided pricing for several optional services. These services are available to the North Carolina WIC program and can be adjusted to suit specific program needs as desired.

Data & Reporting Analyst

Project team members provide a variety of support services for ad hoc database support. Most of these activities are in support of defect and change order analysis. Project staff also provide support for the analysis and preparation of USDA policy related changes. Voyatek understands that North Carolina WIC may also require support for more involved reporting and analysis needs. These could include the preparation of ad hoc reports in Excel, preparation of data for third party entities, or the creation of new SSRS reports to be included within the Crossroads system.

Voyatek can optionally provide staffing to meet these needs with a Crossroads trained data analyst. Voyatek would create an Azure Dev Ops backlog to allow program staff to create research tasks and to track work by the analyst. The analyst would be fully dedicated to producing reporting as needed by the state. Voyatek project team members and technical staff would also be available to provide technical guidance and coordination of complete reporting and analytic tasks.

If the WIC program determines that an ad hoc report should become a standardized report, the reporting analyst would also have the capability to develop new SSRS reports for deployment in the Crossroads system.

Supplemental Development Capacity

The proposed project team is sufficient to meet WIC program requirements for defect management and policy updates. In working with North Carolina WIC, Voyatek has noted that many perfective changes are small in nature. Using a change order process for small changes is inefficient for both Voyatek and North Carolina staff. Voyatek is offering the option to include an additional perfective change developer within the Crossroads project. This developer would be available to complete perfective changes and to contribute to larger change orders. Any hours allocated to the supplemental developer would be removed from the change order costs.

As part of this offer, Voyatek would support the development of a North Carolina mobile application and provide yearly support at no additional cost. The supplemental developer would be allocated to the development and support of the mobile application as needed during the delivery and ongoing maintenance process. Voyatek anticipates that the staff person assigned to this role would be dedicated to North Carolina for most of the contract period. For some time period, Voyatek may propose substituting the staff person assigned to the role to complete specific North Carolina objectives. For example, Voyatek may engage a mobile engineer during

the development of a mobile application. North Carolina could elect to remove the supplemental developer with 30 days written notice.

Mobile Application

Voyatek has developed mobile applications for use by many of our WIC states. Each mobile application is customized to meet state branding and security requirements. Voyatek is providing the option to transfer the WIC on the Web (WoW) mobile application for North Carolina Crossroads use. We are providing two pricing options – one for a standard implementation and one for an option with advanced functions. The standard implementation is used by many WoW states and includes all of the essential functions for a WIC mobile application. North Carolina will have the ability to brand the mobile application using North Carolina specific colors, graphics, food guides and program links.

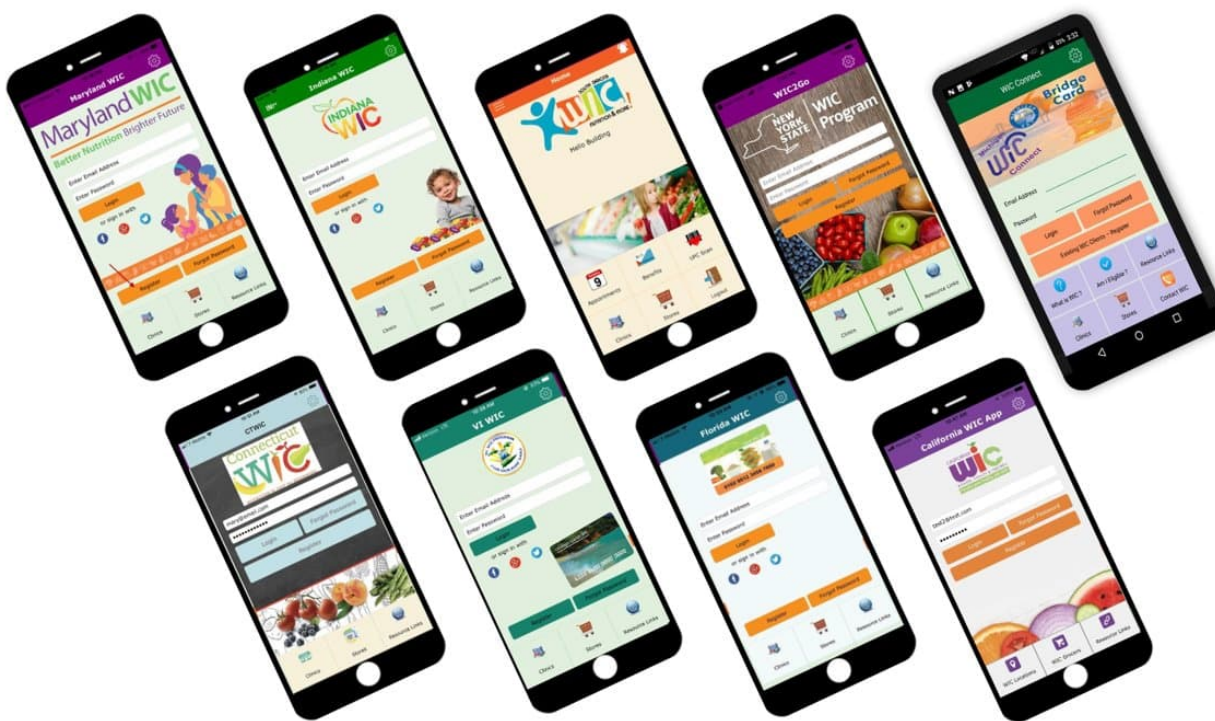


Figure 11: Mobile App Can be Branded Using North Carolina Colors and Images

The decision to use the advanced feature set is often governed by state security policies and balancing ease of access versus application features. For example, some states elect not to allow participants to update and access certain data to prevent triggering state security requirements that would require password changes every 30 days. Voyatek can provide updated costs should a specific feature set be desired that is not shown below.

Standard Implementation

The following capabilities are part of the core WIC mobile application capabilities. These features are available in all systems and would be part of the standard implementation for North Carolina.

- Ability to Login/Register
- Change password
- App Home Screen
- Locate Clinics and Vendors based on zip code or address
- View appointments including what to bring
- View live benefit balance for current and future benefits
- View food guide that describes WIC Eligible foods for each sub-cat
- Scan UPCs in the store to determine WIC eligibility
- Access additional resource materials on the internet as specified by the State
- Push Notifications for appointment reminders, benefit expirations and cert expirations

The project includes the following key activities:

- Transfer the mobile app
- Implement North Carolina branding
- Transfer the service layer and integrate it with the Crossroads server environment
- Implement push notifications
- Coordinate the execution of security scans and address identified issues

Families with active eWIC cards will have the ability to login to the mobile application. Families can create their own login using their email and a custom password that meets minimum complexity requirements. Participant identity is verified by matching their eWIC card number, cardholder birth date, and cardholder zip code with their Crossroads record. Social media logins can also be used if allowed by State policy.

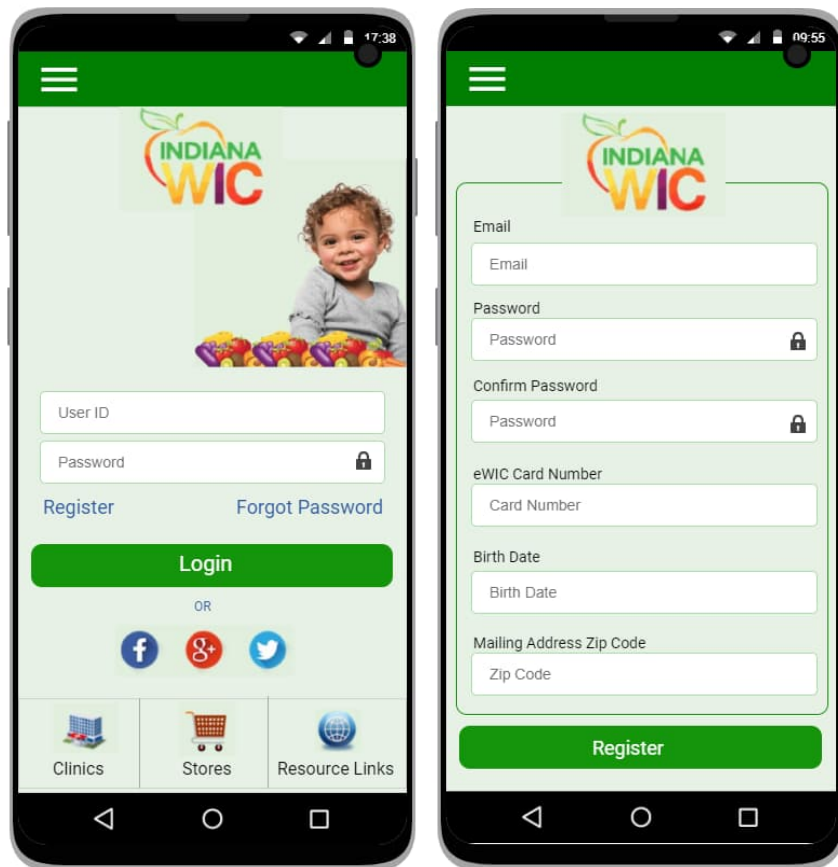


Figure 12: Participants Login or Register on the Mobile App

The system also supports a “forgot login” function that allows users to reset the password linked to the account. The reset process requires the user to provide their email address and the cardholder date of birth.

Clinic and Vendor Locator

The mobile application includes a WIC Clinic and Authorized Vendor locator with the following features:

- Access Clinic information and locate other WIC Clinics around you on the Clinics screen.
- Find out where to shop on the Stores screen.
- Select the help icon on the Stores screen to see the types of stores and products available at each type of store.
- View address and phone number by selecting each pin on the map.
- Maps are interactive – click location name and address popup to quickly call or search for directions
- Expand or limit your search criteria by using the address search or simply by zooming in or out at the bottom of the screen.

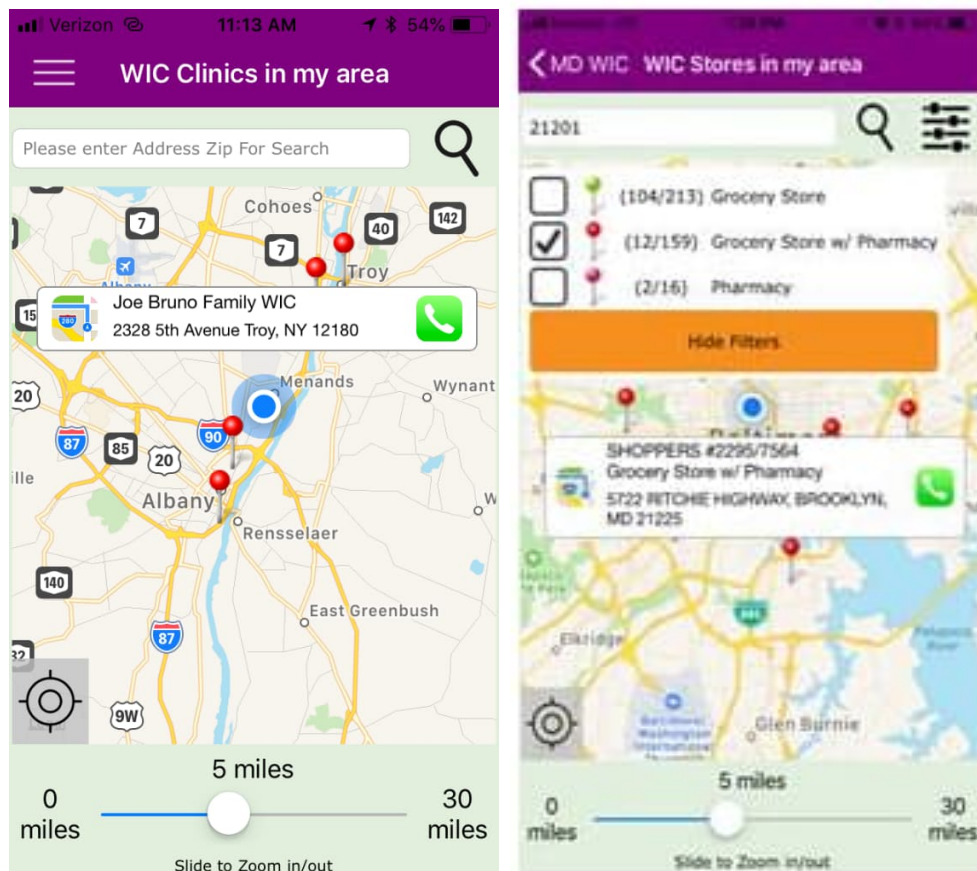


Figure 13: Mobile App Locator for WIC Clinics and Authorized Vendors

Menu and Home Page

The menu and home page include a welcome message for the user and their login name. The mobile application menu will allow users to access the following options:

- Home
- Appointments
- Benefits
- Notifications
- Clinics
- Stores
- Change Password
- Resource Links
- Logout

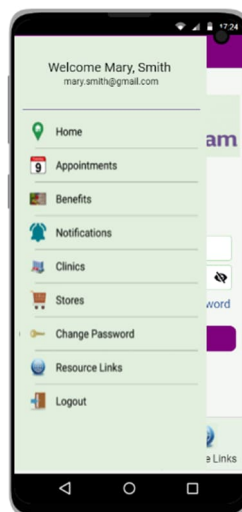


Figure 14: Mobile App Menu and Home Page

Upcoming Appointments

The appointments features allow participants to view upcoming appointments. The appointment details include:

- The clinic where the appointment is scheduled, including telephone number and address.
- Names of each participant in the family who has an appointment scheduled.
- Date and time of each appointment.
- A reminder of what to bring to the appointment for each participant.

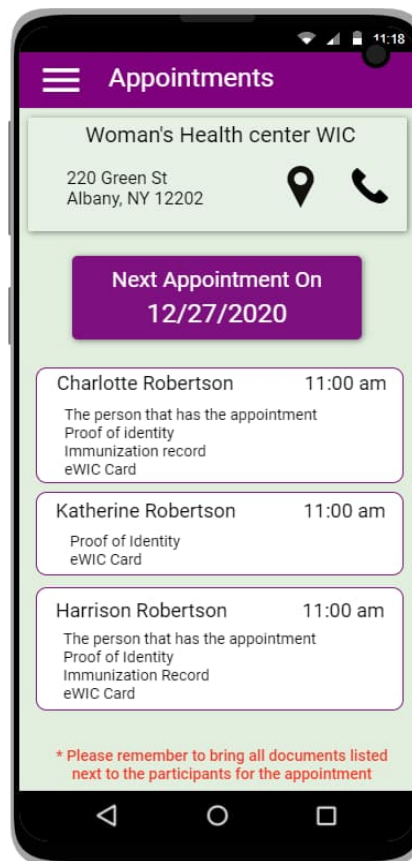


Figure 15: Mobile App Appointments

Benefits

The Benefit Balance screen allows participants to see current and future benefits months. The system provides a visual summary of remaining benefits and allows access to related food guide content from North Carolina's Food Guide. The benefit features include:

- View benefit balance and other benefit information for current and future benefits
- Navigate between current and future benefits using the arrow buttons on the top of the screen, or by swiping left or right
- View details for each food item by selecting the icon
- Sub-cats where all benefits are redeemed are grayed out

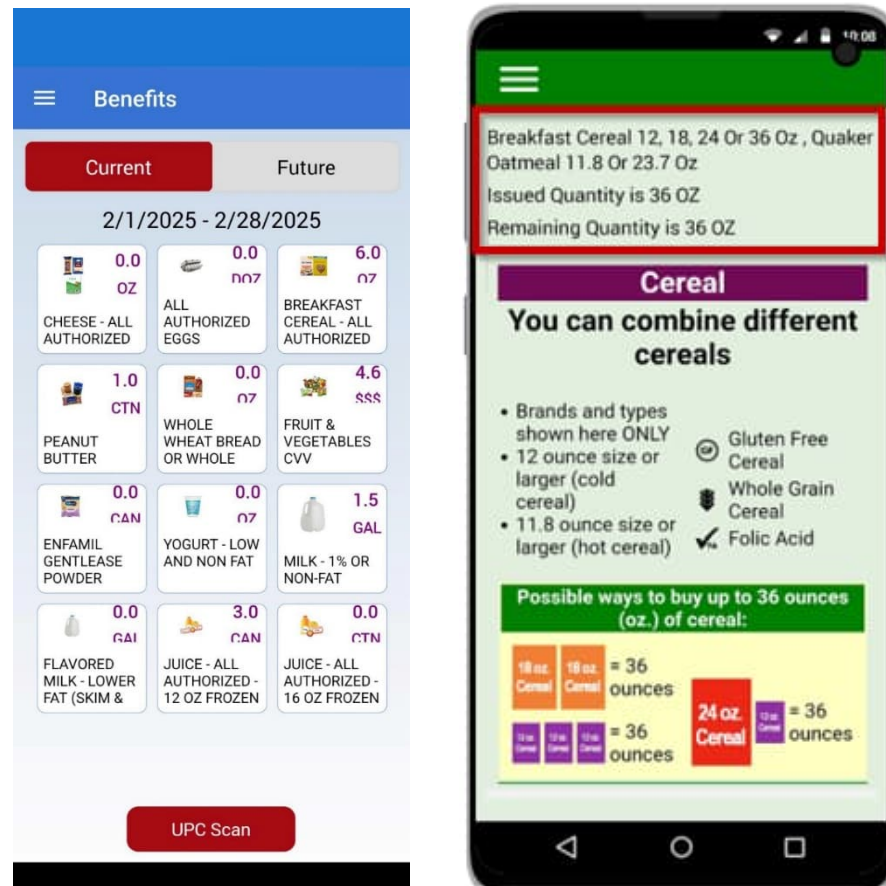


Figure 16: Mobile app Benefit Balance Screens

UPC Scanning

The mobile application includes a UPC scanning tool to allow participants to scan products within the grocery store to determine if items are WIC approved. Once a UPC has been scanned, participants will receive one of the following responses:

- WIC Approved and the remaining balance
- WIC Approved but not on your current benefits
- WIC Approved Zero Balance
- Not WIC Approved

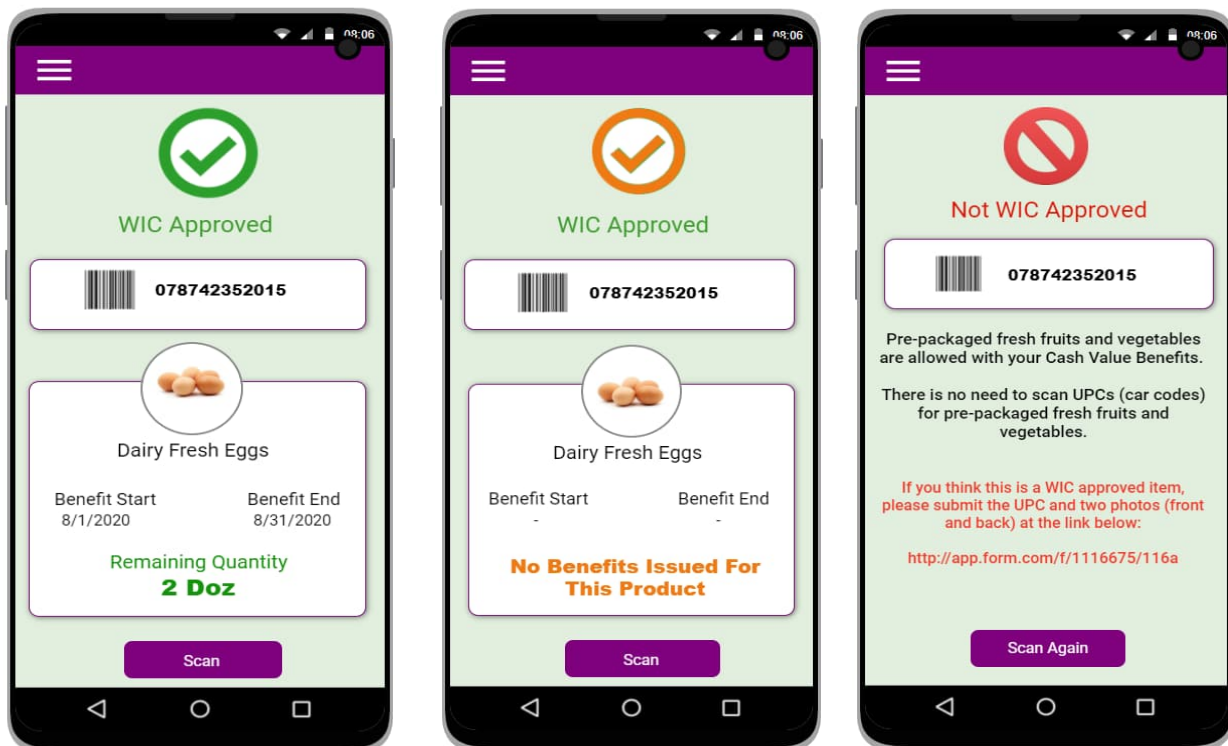


Figure 17: Mobile App UPC Scanning Tool

Resource Links

The WIC mobile application also supports access to North Carolina WIC defined resource links. These links are available without logging and can be used to direct potential applications to appropriate state resources. If desired, resource links can also include contact information for EBT and state-related help desks.

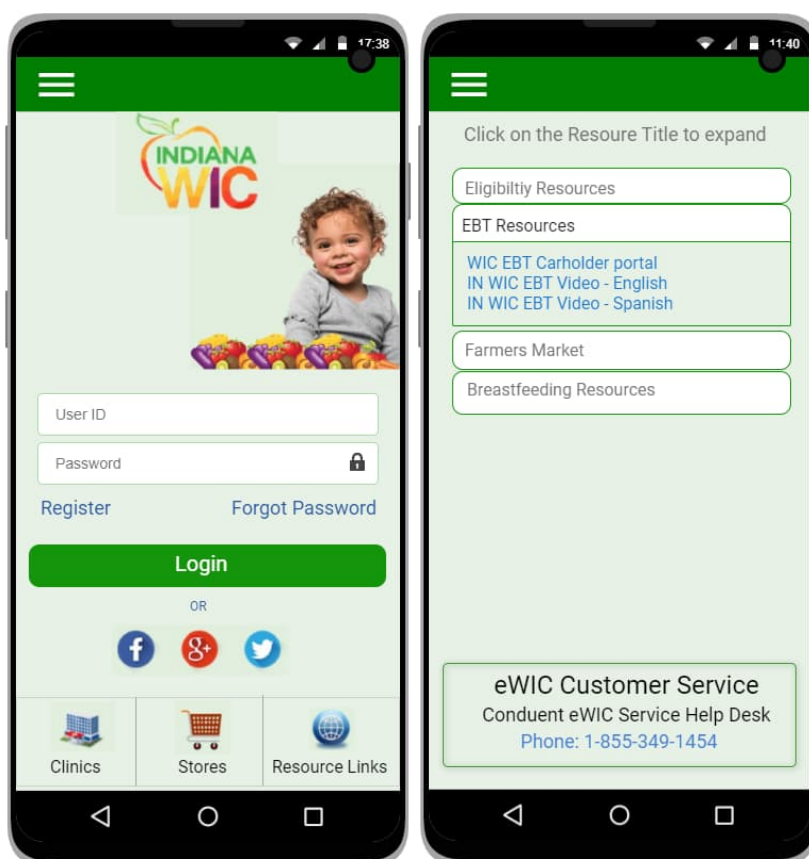


Figure 18: Mobile App Supports Access to North Carolina WIC Resource Links

Push Notifications

The mobile application also supports push notifications to participants. These notifications appear on the participant's phone regardless of whether the mobile application is currently open. Like all mobile applications, the participant must allow the app to send notifications.

Push Notifications are implemented by installing a batch program on the MIS batch server that communicates with the Android and Apple Push Notification Services. The primary function of the program is to send push notifications for appointment reminders. Once the program is set up, it can be easily extended to be used for other scenarios like benefit expiration messages.

These services can be modified during emergencies to support specialized communications related to issues like Covid policy changes, clinic closures, or storm events.

Advanced Options

Voyatek has developed a number of extended mobile application functions that require additional integration with the Crossroads WIC MIS. These features have been implemented in some states but are not common to all state solutions. Voyatek is offering these solutions à la carte so they can be added by North Carolina WIC as desired. The proposed extended features can include any of the following enhancements:

- Upload documents using the mobile app
- Annotate appointments as in-person, phone or video appointments
- Submit new products (UPCs) for WIC's consideration of inclusion into the APL
- View benefit information for multiple cards using the same user account
- Capture electronic signatures
- Display redemption dashboard providing participants access to their shopping history
- Request OTP for password changes
- Create and consume custom nutrition education content

These advanced options are described in further detail on the following pages.

Document Upload

Document upload functions will allow participants to upload required documentation for submission to clinic staff. These documents will be displayed in Crossroads to notify staff of availability and to allow for processing. Participants will have the ability to upload or take a picture of documents as needed. Below are several examples of this potential functionality.

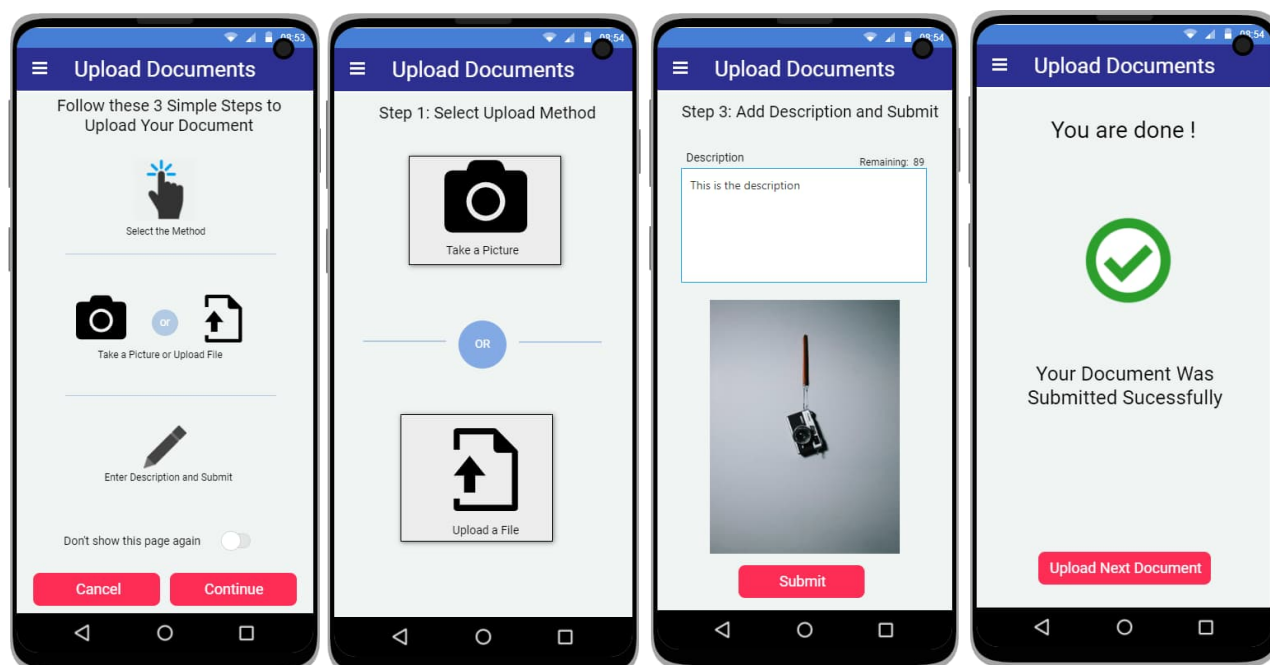


Figure 19: Mobile App Document Upload

Appointment Method Indicator

The appointment method indicator updates the appointment information to include the method of the appointment and to provide integrations with video conferencing services. The system can indicate when appointments are in-person, by telephone or by video appointment. The update is intended to improve integrations with state solutions for video conferencing.

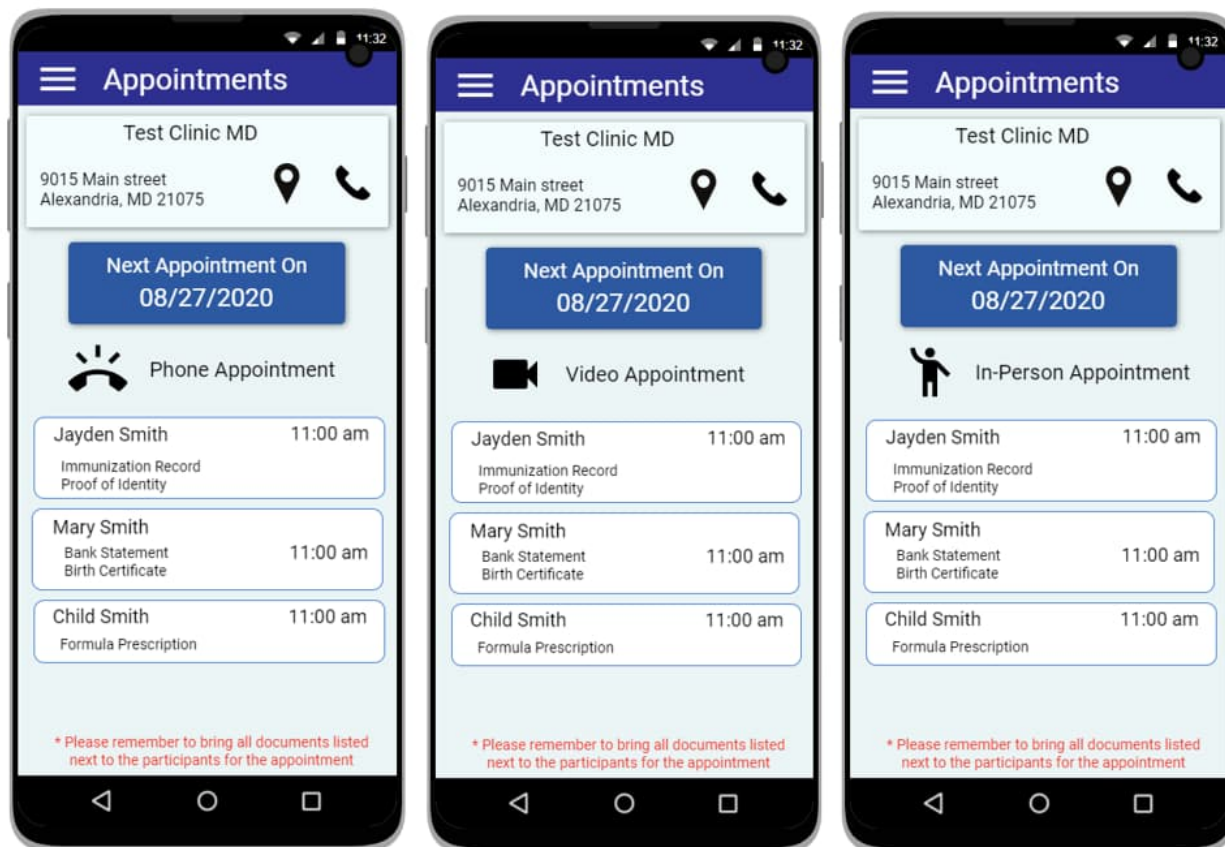


Figure 20: Mobile App Appointment Method Indicator

Product Submission Functions

The production submission tool extends the UPC scanning capability to allow participants to request that products be added to the state's APL. Submission of a product request is integrated with the Crossroads MIS to allow for the review and handling of inbound product requests. This process improves the speed and workflow for participant-recommended products.

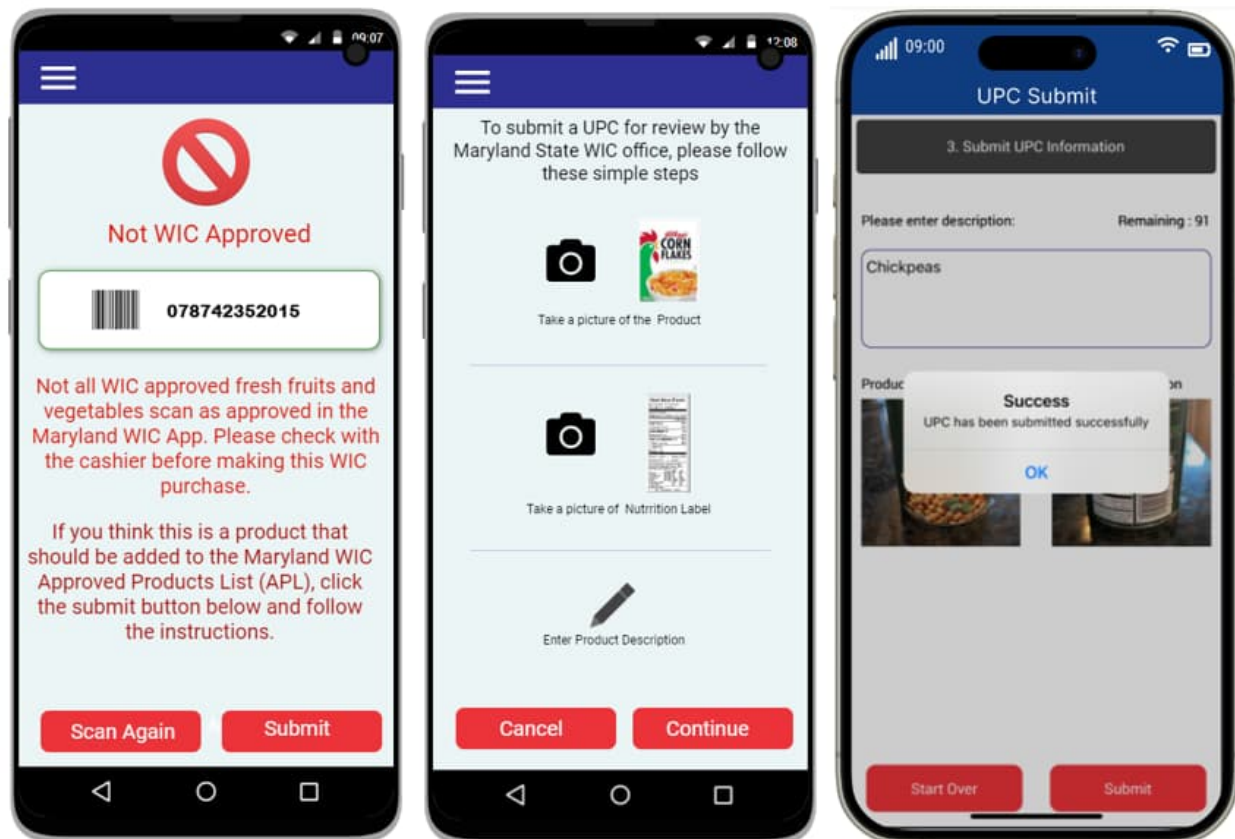


Figure 21: Mobile App Product Submission Functions

Multiple eWIC Card Management

Support for multiple eWIC card management extends the mobile application to allow a single account to access multiple eWIC cards. This is helpful in cases where a caregiver is responsible for multiple foster children that utilize different EBT accounts. This enhancement allows the family member to view balances on each account without having to maintain multiple logins.

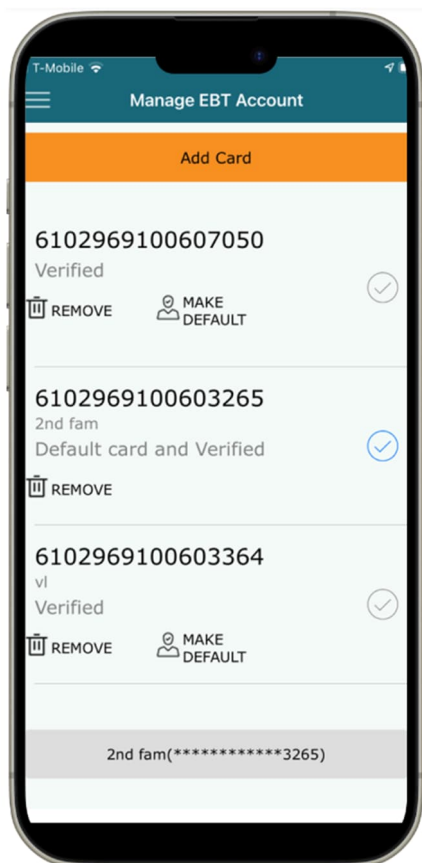


Figure 22: Mobile App Multiple eWIC Card Management

One Time Password Support

This enhancement upgrades the existing login reset based on answering questions with a one-time password sent via email. This enhancement may be desired dependent on state security policies.

Signature Capture

The signature capture enhancement allows staff to request signatures from the Crossroads MIS. Signature requests are visible on the mobile application. Participants are presented with required attestation text and captured signatures are returned to the Crossroads system for processing.

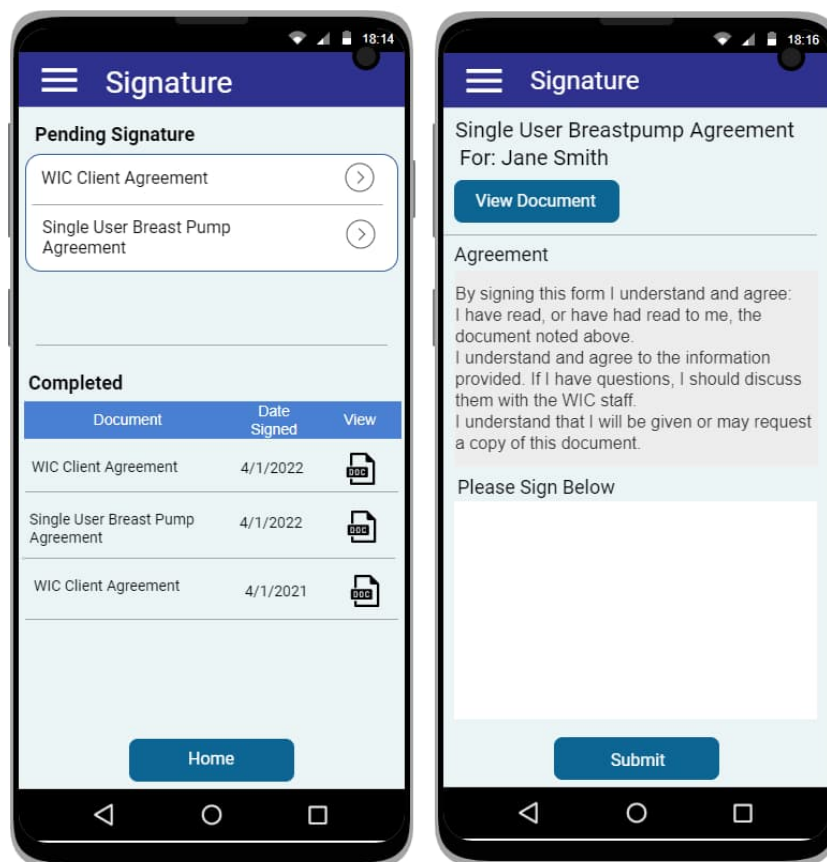


Figure 23: Mobile App Signature Capture

Nutrition Education

The Nutrition Education system adds a nutrition education module within the mobile application. This module can be loaded with state generated nutrition education courses. Participants can view the course library and complete nutrition education courses. Recommended courses for the participant are color coded in the application and course completion will be automatically recorded within the Crossroads MIS.

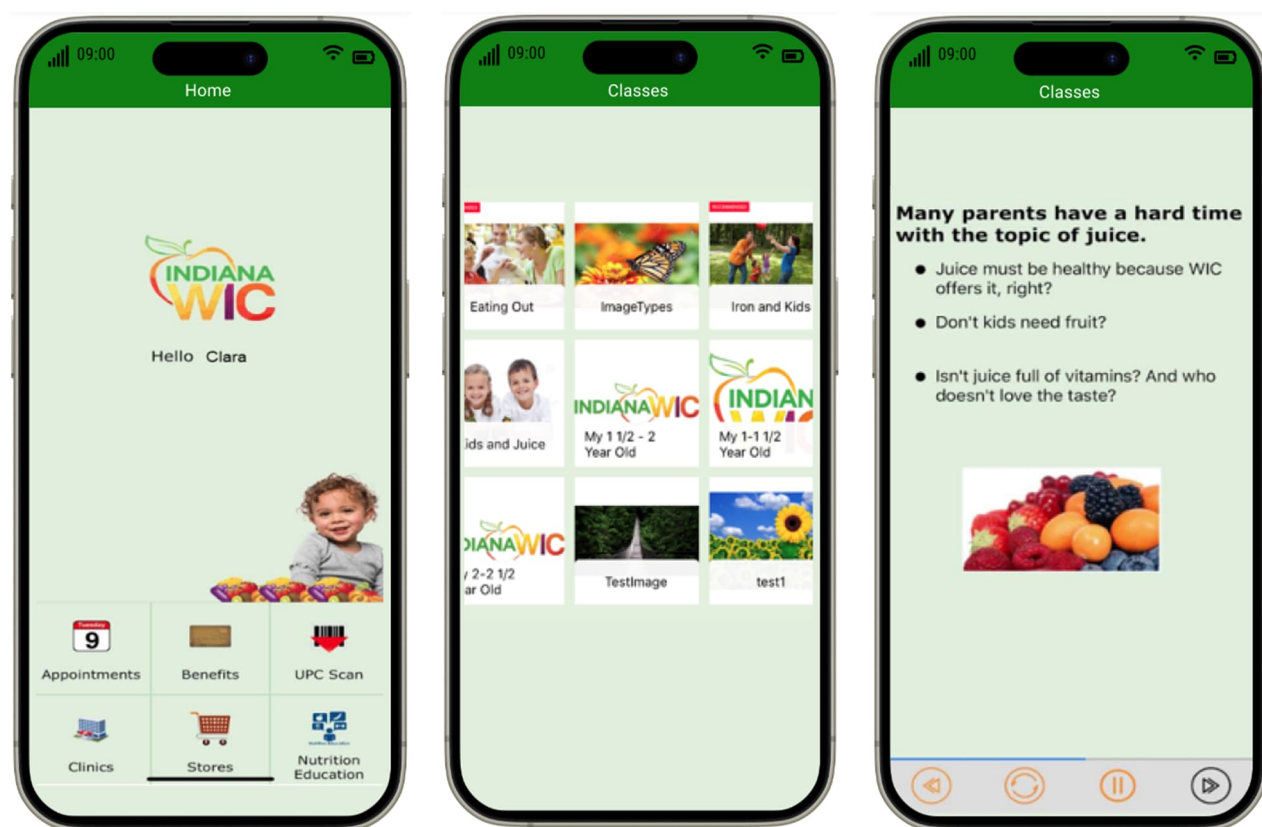


Figure 24: Mobile Application Nutrition Education System

Redemption Dashboard

The redemption dashboard is an information display that provides an overview of redemption behavior. This can include where benefits are redeemed, indicators of redemption percentage in key categories, the percentage of benefits redeemed, and an indicator of the value of benefits redeemed. The goal is to encourage redemption and reinforce the economic benefits of WIC participation. This dashboard can be customized based on state priorities and guidance.

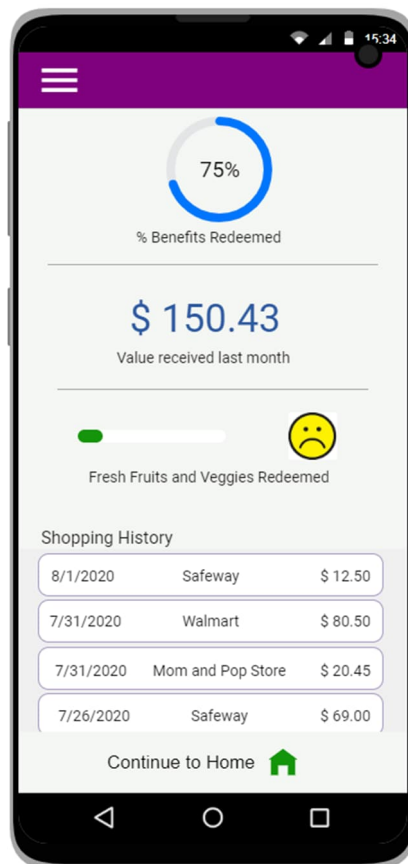


Figure 25: Mobile App Redemption Dashboard

Farmers Market

The eFMNP Project was initiated by Georgia WIC last year to replace paper coupon issuance and manual farmer banking processes. The enhancement includes several key components:

- Farmer Registration and Market Assignment, which streamlines the enrollment of farmers and their market placements
- Participant Registration and Benefit Issuance, ensuring efficient distribution of benefits
- eFMNP Mobile Application, providing users with a digital platform for transactions
- Reconciliation and Reporting, enabling accurate tracking and financial oversight
- Season Configuration, allowing for flexible program adjustments based on seasonal requirements

The mobile application is available on both iOS and Android platforms and is a feature-rich and intuitive tool designed to streamline operations for registered farmers. It enables them to easily accept digital benefits and track transactions in real time.

Georgia farmers who used the app during the 2024 farmers' market season praised its user-friendly design and financial features, which helped them efficiently track transactions and manage operations throughout the season.

The mobile app offers the following functions:

- Choose a market location for business
- Verify eligible participant benefits
- Record purchases
- View transaction history
- View payment history
- View total sales by day and monthly sales to date

The Home screen provides quick reference information for the farmer and serves as the starting point for new sales transactions when a participant presents the food items they wish to purchase and their EBT card. WIC participants use their existing EBT cards, as the app is equipped with Optical Character Recognition (OCR) functionality, allowing it to automatically read the card number without the need for additional QR code stickers to identify the family.

The app allows the farmer to select their market location and modify it if they travel to a different location for transactions. This confirms that the market location is accurately recorded for proper reporting.

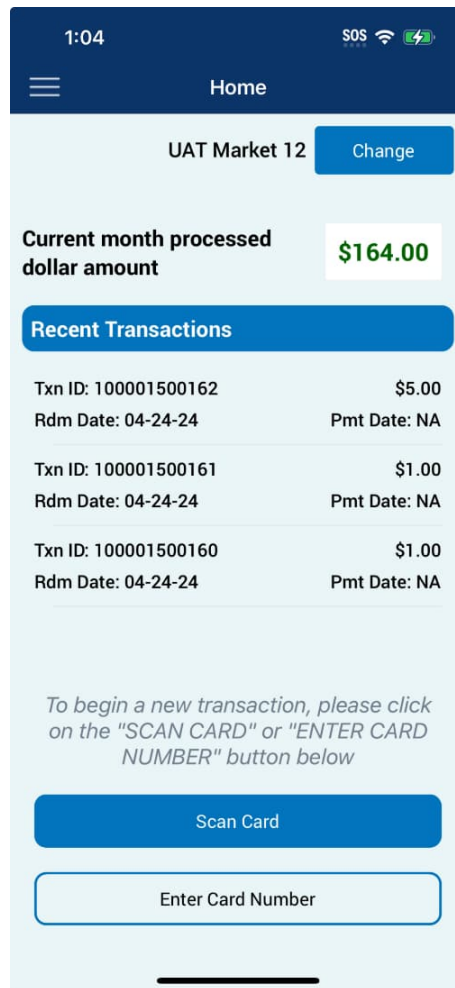


Figure 26: Farmers Market Home Screen

Once scanned, the system displays the participant's available balance and allows the farmer to enter the items purchased along with their prices. If the total exceeds the available balance, the farmer is notified, and the participant can choose which items to purchase.

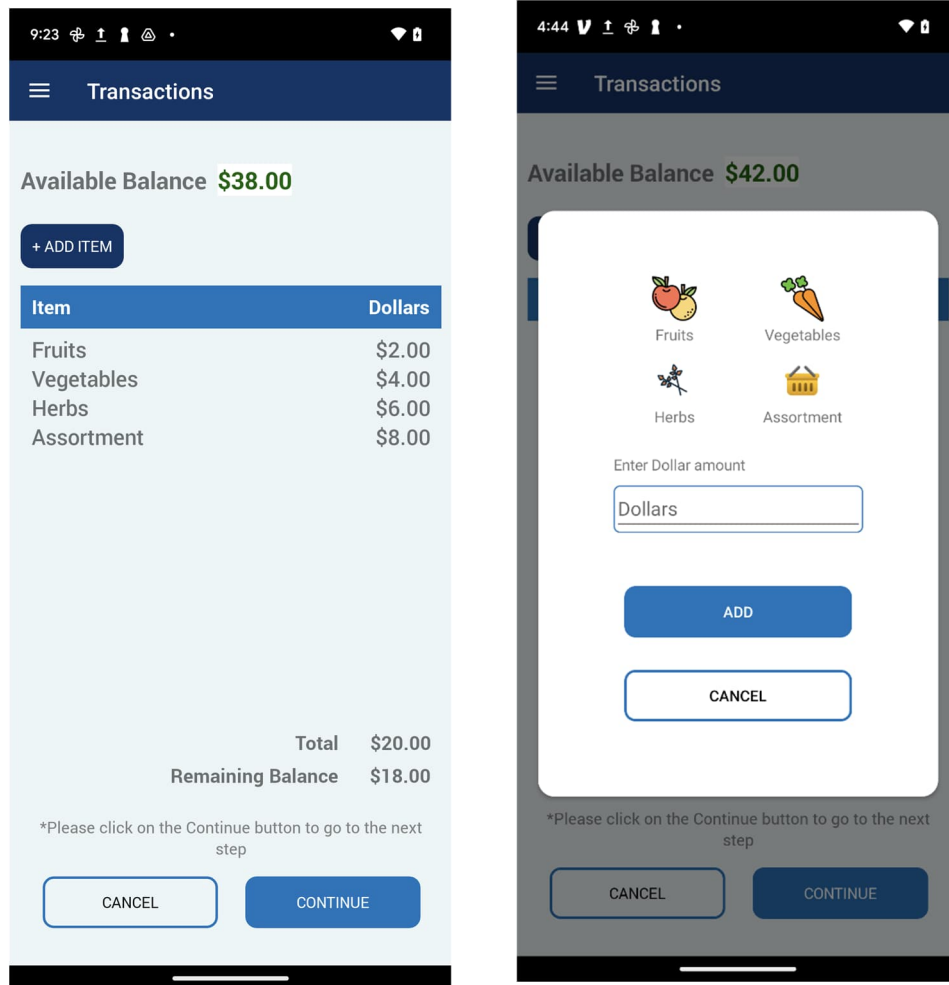


Figure 27: Farmers Market Available Balance

The Summary screen shows the descriptions and prices of the items being purchased. Sales cannot be completed until the participant provides their signature for acknowledgment. Once the sale is processed, a confirmation screen appears to notify the farmer of a successful transaction. If any issues arise, the farmer will receive instructions on how to proceed.

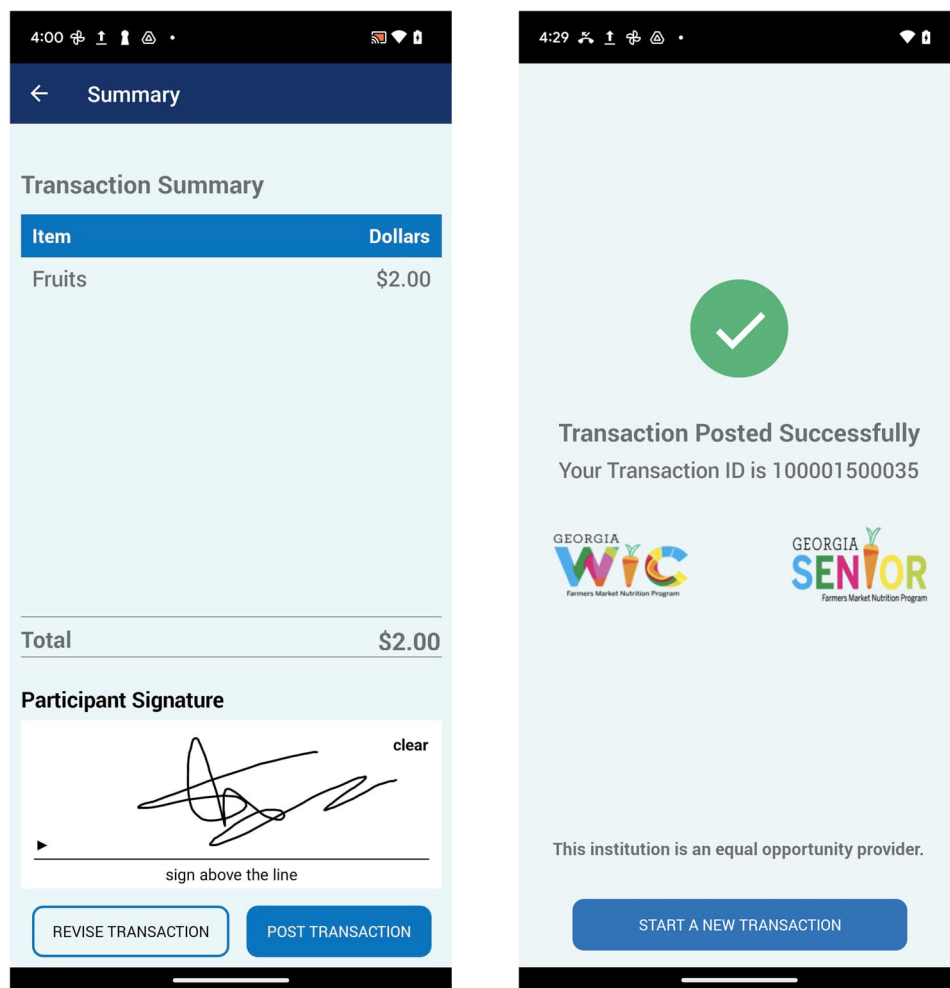
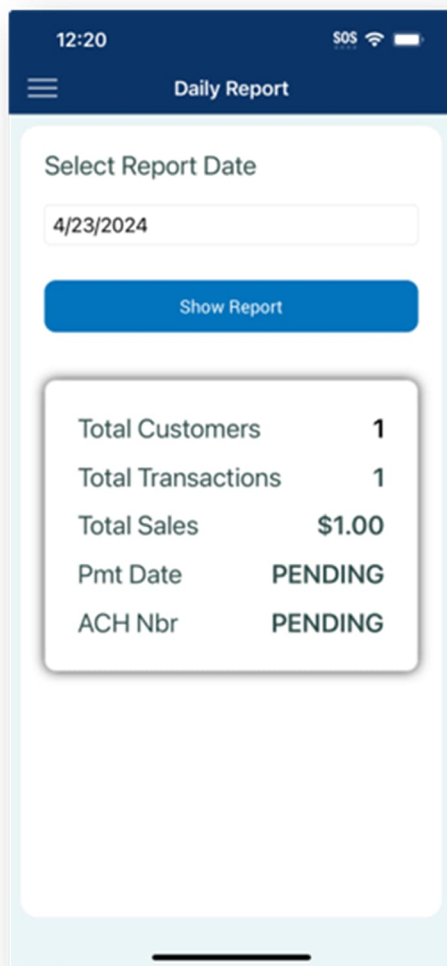


Figure 28: Farmers Market Summary Screen

The app provides the farmer with a daily report that displays the total number of customers served on the selected date, the total transactions, the total sales amount, the payment date, and the corresponding ACH payment number. If the ACH has not been processed yet, both the payment date and ACH payment number will display as "Pending."



Total Customers	1
Total Transactions	1
Total Sales	\$1.00
Pmt Date	PENDING
ACH Nbr	PENDING

Figure 29: The Farmers Market Daily Report

The mobile app is equipped with robust security features to assure data protection, including a requirement for login credentials and the expiration of passwords every 30 days. Farmers must provide confidential information during registration to access the app. Passwords are required to be between 8 and 20 characters in length and must contain at least one uppercase letter, one lowercase letter, and one number. Additionally, new registrations must be authorized by WIC or FM staff before they can be used. To maintain security, WIC or FM staff also have the authority to deactivate mobile users when necessary.

Farmers are reimbursed via automated clearing house (ACH) payments making this solution completely paperless.

Georgia's eFMNP solution offers the same features to manage the Senior Farmer's Market Program, providing similar functionalities for tracking transactions and managing benefits.

The solution also provides the following reports:

- WIC and Senior Financial Reports
- WIC and Senior Participation Reports
- WIC and Senior Reconciliation Reports
- WIC and Senior Redemption by Vendors
- WIC and Senior Agency Listing Reports
- WIC and Senior Monthly Redemption by Agency
- WIC and Senior Monthly Redemption by Vendor
- WIC and Senior Benefit Summary Reports
- WIC and Senior Unused Benefit Reports
- FMNP and SFMNP Financial and Program Reports-
- Farmers Market Program Data Summary Report (683 A and B)
- ACH Transactions by Farmer
- Total ACH payments by Farmer
- Total ACH payments by Date
- Transactions by Date
- Daily ACH by Program

Penetration Testing

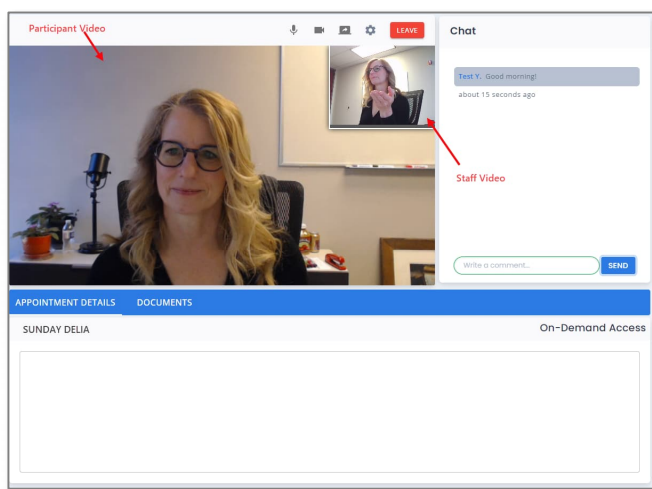
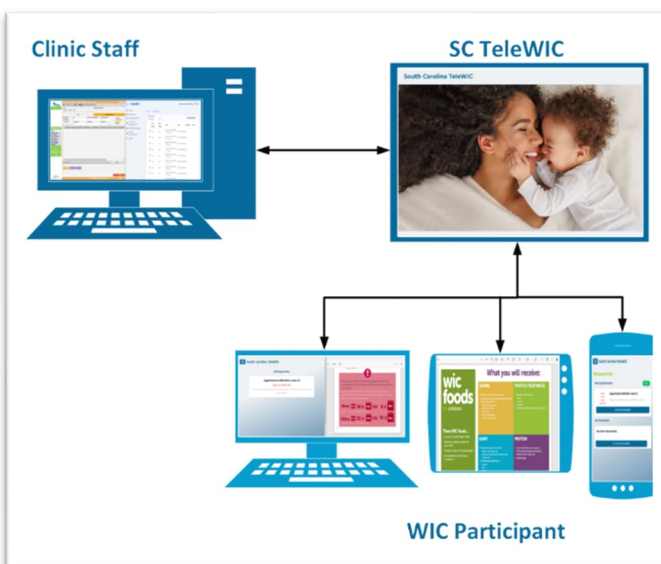
Voyatek can optionally hire a third-party to perform a penetration test against the North Carolina hosting environment. Third party penetration testing is sometimes requested to verify network security for production systems. The test report would be available to North Carolina WIC and IT staff and the resolution of any identified issues would follow normal contract terms and conditions.

TeleWIC / Two-way Texting

Voyatek is offering as an optional service our **TeleWIC telehealth communication system**. TeleWIC is a full-featured, modern, cloud-based product that can connect to any WIC MIS based on the defined application programming interface (API). TeleWIC enables participants to connect to a clinic and WIC staff at an appointed time and to participate fully in their WIC appointment without having to pack up the kids and travel. TeleWIC extends WIC's reach, provides flexibility, and facilitates high-quality interaction with participants almost as if they were in the clinic.

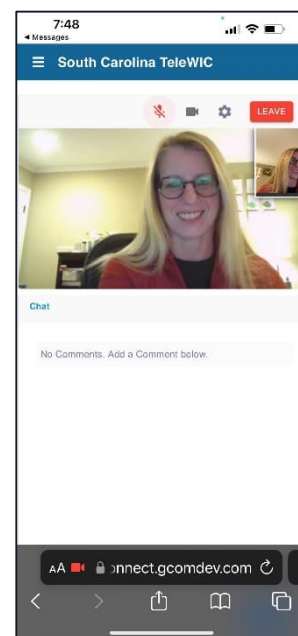
TeleWIC Features

- Integrated TeleHealth for WIC MIS
- High-quality video appointments
- Cloud hosted Software as a Service (SaaS)
- Integrate with state identity provider
- Flexible setup and configuration
- Branding and customization
- Phone, tablet, or desktops
- Defined API for any MIS integration
- All browsers – Apple, Android, Google, Windows
- Licensed based on needs of state agency



TeleWIC Call

- Video call
- Chat window
- Ability for 2+ provider staff
- Access to participant data
- Screen sharing
- Document sharing & assignment



In addition to offering the TeleWIC integrated platform, Voyatek is also offering the underlying services to allow for Video Conferencing and Two-Way Texting integration with the existing Crossroads portal. Pricing for services is volume based and can be used to implement these services within existing applications.

TeleWIC – Provider Portal

- Agency can define Rooms and Room Groups
- Support for scheduled and on-demand appointments
- Users are assigned access to Room Groups
- Text and Email messaging
- Create documentation libraries
- Dashboard for monitoring upcoming, waiting, and in progress calls
- Multiple providers can join call
- Ability to share documentation
- A participant joins a call a defined number of minutes before call (waiting room)

TeleWIC – Participant App

- Multiple authentication methods for participants
- State-defined identity verification
- Access to upcoming appointments
- Access to on-demand services
- Access to assigned documents
- Text and email notifications using agency defined templates

Appendix S: Key Personnel Resumes

M&E Vendor Product Manager – Jennifer Saunders

Jennifer Saunders' resume follows.

Jennifer B. Saunders

Project Director

Over 25 years' experience providing services in government sector, specializing in social services with over 12 years' successfully delivering, managing, and coordinating software implementation projects with recognized strengths in account management, risk analysis and mitigation strategies, budget, and schedule management, planning and documentation, and execution. Expertise in managing statewide MIS implementation projects with additional experience delivering citizen engagement management systems for 311 Services to transform people-heavy services to digital online services for the management of service requests including streamlining processes for staff, improving the customer and citizen experience interacting with their local government, and providing better data on service delivery and customer satisfaction to facilitate improvements in responsiveness and customer satisfaction.

Voyatek (formerly GCOM Software LLC)
April/2018 – Present

Sr. Project Manager, North Carolina Maintenance and Enhancement Services for the Crossroads WIC Management Information System
July/ 2021 – Present

- Served as the primary point of contact for the contract and project for North Carolina WIC
- Provided contract administration and project management throughout the contract
- Developed project plans and objectives, ensuring technical feasibility and involving all relevant stakeholders
- Oversaw resource availability and allocation, ensuring timely development of project deliverables within scope and budget
- Measured project performance using appropriate systems, tools, and techniques, and managed changes in project scope, schedule, and costs
- Managed relationships with North Carolina WIC, stakeholders, and third parties/vendors as needed
- Performed risk management to minimize project risks and created/maintained project management documentation

Sr. Project Manager, South Carolina Department of Health and Environmental Control (SC DHEC), WIC
April/2018 – October/2024

- Sole project manager accountable for the transfer, hosting, and state-wide implementation of the SCWIC MIS system for the SC DHEC Women, Infant, and Children (WIC) program including data conversion, software development, interface development for EBT and Medicaid, data extracts and file movement for external consumption, and conducting training for all testers, super users, and end users.
- Performed cross-team management of 25+ team members located in 3 states

Subject Matter Expertise

- Project Management
- Health and Human Services
- At-Risk Project Management

Education

- MA, Human Development and Family Life, University of Kansas (1997)
- BA, Human Development and Family Life, University of Kansas (1992)

Professional Certifications

- Project Management Professional (PMP)® - Project Management Institute (PMI), 2012
- Board Certified Behavior Analyst BCBA) - BACB, 2003-2009

- Managed and supervised the day-to-day activities of developers, quality assurance, trainers, business analysis, and IT staff to ensure deliverable completion according to contract requirements and quality standards.
- Successfully managed and delivered branded and enhanced MIS software releases, mobile app, onsite training for UAT, Pilot and Rollout, procured training locations, coordinated training logistics for four-month statewide Rollout, managed and provided onsite training and support for UAT, Pilot readiness, Pilot Go Live, Rollout readiness and Rollout Go Live.
- Successfully transitioned to system operations and maintenance two months ahead of schedule.
- Established and maintained relationships and open communication with Key Client Stakeholders including third-party QA and EBT contractors, and supported state reporting to USDA Food and Nutrition Services.

Sr. Project Manager, California Department of Public Health, WIC
October/2020 – June/2021

- Sole project manager accountable for completion of System Acceptance for the state-wide implementation of the WIC WISE MIS system for the California Department of Public Health Women, Infants and Children (WIC) program.
- Performed cross-team management of 35+ team members located in 5 states.
- Managed delivery of system enhancements, maintenance and support services, system acceptance and project closeout deliverables, contract management including managing and coordinating sub-contractors, and negotiations for Maintenance and Operations contract amendment.

Verint Systems, Inc.
January/2015 – April/2018

Solution Delivery Manager, North American Government Engagement
January/2015 – April/2018

- Manage North American and global client accounts, responsible for customer satisfaction and managing accounts including hosted and on-premise customers of CRM system and citizen mobile application.
- Oversee the delivery of multiple concurrent projects (Governance), ensuring successful delivery and client satisfaction.
- Line manager to members of the North American Professional Services team, mentoring and maximizing staff potential.
- Support new and existing customer sales, shaping solution proposal, building estimates, writing RFP response, and pre-sales consultancy (solution/delivery).
- Accountable for the delivery of the largest and most challenging projects and managing projects with multiple work streams.

Sr. Project Manager, Los Angeles County Department of Public Social Services
May/2016 – January/2017

- Managed projects to a statement of work (SoW) within time, cost and quality parameters including management of and reporting on risks, and resources.
- Established and maintained relationships with Key Client Stakeholders.

- Strove to improve processes & solutions; mentored and supervised project managers with demonstrated ability to 'turn around' projects with significant issues.
- Managed resources effectively to ensure highest possible customer satisfaction and project outcomes).

Computer Science Corporation (CSC)

August/2006 – December/2014

Sr. Project Manager, Missouri Department of Health & Senior Services WIC, Montana Department of Public Health and Human Services WIC, Mississippi State Department of Health WIC

January/2008 – December/2014

- Sole project manager for three consecutive statewide project to transfer and implement the SPIRIT MIS system; projects ranged in size from \$1.5 million to \$2.6 million. Point of contact for the customer and project stakeholders; managed and maintained positive customer relationship during implementation and through initial year of maintenance and operations.
- Managed project schedule and report project status; wrote and managed to various project plans; managed and controlled budget.
- Created and executed Project Management Plan including such subordinate plans as Communication, Risk Management, Security, Configuration Management, Disaster Recovery, Implementation and Help Desk Support.
- Managed team of 10+ staff including developers, quality assurance analysts, business analysts, trainers, IT and DBA staff, and help desk staff to achieve customer objectives.
- Supported sales and marketing responses to various new business opportunities, analyzing requirements, developing delivery strategy, estimating effort, preparing, and writing response documentation.
- Supported an Agile software development project by facilitating detailed requirements review sessions and managed completion of several requirements documents for the primary care management module.

Business Analyst / Trainer, Chickasaw Nation WIC

August/ 2006 – December/2007

- Managed and documented business requirements for a USDA funded software development project for a 10-state consortium; created change orders documenting requirements, system designs with sample graphical user interfaces, process flows, algorithms, and system edits
- Facilitated design discussions with the customer, regulatory stakeholders, and technical staff; conducted design walkthrough sessions for customer acceptance
- Conducted training for user acceptance testing and statewide rollout; provided on-site support to the customers during UAT, pilot and statewide rollout
- Instrumental in developing a system playground for potential customers to experience and learn about our product

Johnson County Developmental Support (JCDS)

June/1997 – August/2006

Behavior Support, Alternative Support, Live Skills Support Coordinator

June/1997 – August/2006

- Managed and documented business requirements for a USDA funded software development project for a 10-state consortium; created change orders documenting requirements, system designs with sample graphical user interfaces, process flows, algorithms, and system edits
- Facilitated design discussions with the customer, regulatory stakeholders, and technical staff; conducted design walkthrough sessions for customer acceptance
- Conducted training for user acceptance testing and statewide rollout; provided on-site support to the customers during UAT, pilot and statewide rollout
- Instrumental in developing a system playground for potential customers to experience and learn about our product

M&E Vendor Development Manager – Michael Heinrich

Michael Heinrich's resume follows.

Michael Heinrich

Software Developer II

Software Engineer with 20 years demonstrated history of working in the computer software industry. Strong full-stack business development professional skilled in C#/.NET, EF, HTML, CSS, MS SQL, Oracle, Bootstrap, jQuery, LINQ, WordPress, MySQL, and Python.

Voyatek (formally GCOM Software LLC)

October/2019 – Current

Software Developer, North Carolina WIC
August/2022 - Current

- Developed Telehealth client portal website as part of the North Carolina WIC team utilizing C#, MVC.Net, HTML5, CSS3, jQuery, Bootstrap, and MS SQL.
- Implemented accessibility standards for ADA compliance for Telehealth.
- Standardized style and layout for site to achieve consistency across all pages.
- Develop new and update existing APIs.
- Implemented data import from Telehealth to existing Crossroads application utilizing VB.Net, WPF, and Entity Framework.

Senior Programmer Analyst, The State of Maine

October/2019 – August 2022

- Developed full stack Enforcement System (ES) for the Department of Environmental Protection using MVC.Net, Oracle, and Entity Framework.
- Developer user guide for ES System.
- Maintain and enhance public facing and internal websites and windows services for the Public Utilities Department.
- Developed SSRS reports for the Department of Agriculture.

Insurance Technologies Corporation

June/2016 – March/2019

Programmer/Analyst, Insurance Technologies Corporation

June/2016 – March/2019

- Developed real-time Leads Dashboard for web-base, multi-tenant comparative rating application (TurboRater) using SignalR, SqlDependency, and RESTful APIs.
- Designed and developed proof of concept application for TurboRater to introduce responsive UI and replace third party controls.
- Developed enhancements to TurboRater using C#, Kendo UI, MS SQL, and .Net.

Farm Credit Bank of Texas

October/2012 – August/2015

Subject Matter Expertise

- Web Development
- SQL Development
- Technical Writing

Education

- BA, RTVF, University of North Texas.
- BA, CIS, University of Maine at Augusta (complete in 2024)

Software Development Engineer, Farm Credit Bank of Texas
October/2012 – August/2015

- Responsible for maintenance and enhancements for FCBT Associate credit union member's websites (16 organizations at the time) utilizing C#, ASP.Net, PHP, VB, Photoshop, MS SQL, and MySQL.
- Developed Site Bridge, an in-house CMS website utilizing, C#, ASP.Net, Entity Framework, and MS SQL that allowed the credit unions to update content (text and images), layout, scheduled notification messages (such as outages), and restrict access to their online banking portals.
- Working with the marketing department, converted most Association member sites to responsive applications.
- Implemented Shared Configuration to IIS production servers.
- Implemented SQL Server migration using SSIS.

M&E Vendor Test Manager – Helena Young

Helena Young's resume follows.

Helena Young

Senior Consultant- Tester III

Senior Quality Assurance professional with extensive experience in testing software solutions and migrating data into new solutions. Successfully meets deadlines and delivers solutions on time and within budget. Extensive work experience in System Testing, User Acceptance Testing (UAT), Functionality Testing, Black Box Testing, Integration Testing and Regression Testing. Expert in Data Conversion, application testing, and back-end testing.

Experience

- Experience testing SQL, JAVA, AMDOCS, ORACLE 9i, VB and .NET applications.
- Expert in Defect Management using Change Synergy, Bugzilla, Jira, TFS and Zephyr.
- Collaborates with functional teams through the design, implementation, and testing and deployment process.
- Experience with Agile and Waterfall development methodologies.
- Writes SQL queries to verify data in MS SQL Server databases.
- Provides support to management with project planning, coordination and implementing various QA methodologies.
- Prepares and executes test plans and test cases.
- Expert in planning and executing Functional Testing, Data Validation, Compatibility Testing, Regression Testing, Integration Testing, Link testing and Negative Testing.
- Expert using Quality Center and Test Director
- At ease in high stress environments which requires the ability to multi-task
- Proven ability to work efficiently in both independent and teamwork environments
- Performed Manual Testing and Automation Testing using Mercury Interactive Tools such as Win Runner, Load Runner, and Test Director
- Generated user scripts and load scenarios using Load Runner for different transactions to execute Load Testing, Stress Testing and Acceptance Testing

Technical Skills

- Platforms : MS-DOS, Windows, UNIX, Linux
- Databases : SQL, Oracle, MS SQL Server, MS Access.
- Reporting Tools : Actuate, Change Synergy, JIRA, Quality Center, Zephyr, TFS

Subject Matter Expertise

- Expert in Defect Management
- Experience testing SQL, JAVA, AMDOCS, ORACLE 9i, VB and .NET applications
- Expert in planning and executing Functional Testing, Data Validation, Compatibility Testing, Regression Testing, Integration Testing, Link testing and Negative Testing
- User scripts and load scenarios using Load Runner

Education

- BS Business Management Friends University
- AS Computer Science Donnelly College

Professional Certifications

- Fred Pryor Project Management Certification
- Sprint National Management Certification

Accomplishments

- Sprint Quarterly Top Performer Award, Sprint Extra Mile Award, Sprint Outstanding Customer Service Award, Sprint President Club Award

- Billing : Amdocs, Convergys
- Languages : Shell Scripts, SQL, VICORP, Brite Voice IAS, Basic, COBOL
- GUI : Developer 2000, Visual Studio 6.0
- WWW : HTML, XML, JavaScript, and ASP
- Methodologies : Agile, Waterfall
- Testing Tools : Mercury Interactive (Win Runner, Test Director, Load Runner and QTP), EMPRIX, RATIONAL Tools.
- Visual Modeling : UML with Rational Rose 98/2000.

Professional Experience

Voyatek (formerly GCOM Software LLC, 3Sigma WIC

May/2019 – Current

Sr Consultant, Tester III, Crossroads WIC (Women's Infants and Children) Application for - North Carolina

DXC Technology

2011 – May/2019

Senior QA (Lead) and Data Conversion Testing Lead, Crossroads WIC (Women's Infants and Children)

Application for Alabama, North Carolina, Virginia, West Virginia

Segue Technologies

2009 – 2011

Senior QA (Lead) and Data Conversion Testing Lead, Crossroads WIC (Women's Infants and Children)

Application for Alabama, North Carolina, Virginia, West Virginia

Sprint IT Call Center Services

2007 – 2009

QA (Lead), Telecom billing software AMDOCS Ensemble (Supports Telecom Customer Care, Billing)

Sprint IT Enterprise Test

2004 – 2007

Senior QA (Lead), Sprint Relay platform (Accessibility)

Sprint PCS –ITS Service Delivery

2000 – 2004

Project Manager IV, Sprint Business Migration Project for Customer Care, Logistics and Billing. Migration System solution to deliver committed financial synergy

Sprint Enhanced Services

1994 – 2000

Sr. Technical Consultant, Sprint product enhancements for, IVR Enhanced Interactive Toll-Free Services and Call Center Services

M&E Vendor Business Analyst Manager – Cindy Kochersperger

Cindy Kochersperger's resume follows.

Cindy Kochersperger

Business Analyst III

Business Analyst professional with over 30 years of experience in the Information Technology (IT) industry beginning as a developer which provides a technical background. Consistently delivers quality projects on time with a high degree of customer satisfaction. Excellent interpersonal and communication skills enhance external and internal relationships to ensure positive outcomes. Over 9 years developing and supporting WIC Nutritional program systems across five states. Over 25 years supporting the health and medical industries and over 12 years supporting various government programs including WIC, State Courts Administration and State Department of Revenue.

Voyatek (formally GCOM Software LLC)
September/2018 – Current

Subject Matter Expertise

- Business Analyst Management
- WIC Software Development
- Application Development

Education

- BS, Mathematics and Computer Science, University of Central Missouri (1980)

Business Analyst, North Carolina WIC
April/2019 – Current

- Oversee all project work for North Carolina WIC M&O contract, providing Business Analyst support across all modules
- Delivered all state-requested releases on time with minimal UAT issues
- Improved the deployment process using Octopus, allowing deployment to any environment within several hours
- Gather requirements and author all change request documents for the NC project
- Deliver all release-specific documents and documentation for production deployments
- Supported the transition of Vendors to a new peer group structure
- Improved the Note To Exceed (NTE) calculation process to run in minutes (previously had taken days to complete)
- Provided guidance and solutions to support all COVID-related waivers
- Designed and management development of a mobile-accessible website for the Telehealth participant portal

Business Analyst, New York WIC
September/2018 – April/2019

- Part of training team to deliver Train-the-trainer sessions for NY WIC rollout (WOW software)
- Business Analyst and QA activities for improvements to the MYWIC mobile application
- Business Analyst and QA activities for development of CARA (tablet-based Vendor Monitoring system for WIC)

Teva Pharmaceuticals
April/2016 – September/2018

Business Analyst, Teva Pharmaceuticals

April/2016 – September/2018

- Developed protocol and supervised team of twenty nurses to review past virtual health conversations to identify missed reporting 'adverse affects' to FDA. Performed data analysis and reporting
- Authored SOP for SOPs for Patient Services and Solutions and performed training to staff
- Business Analyst activities to support Patient Services and Solutions software, including transition from custom systems to Salesforce.

DXC Software

September/2011 – April/2016

Business Analyst Manager, DXC Software

September/2011 – April/2016

- Managed team of four business analysts on WIC Crossroads development and maintenance (a large, multi-year, multi-state project to develop a system to administer WIC Nutritional Program)
- Provided Business Analyst activities specializing in EBT, Administration and Caseload
- Provided onsite support at multiple consortium states during UAT
- Developed and maintained documentation and training documents
- Functioned as account manager for the first state to go live with Crossroads

Clinical Reference Laboratory and GE Insurance Solutions
2004 – 2011

Business Analyst, Clinical Reference Laboratory and GE Insurance Solutions

2004 – 2011

- Project management for large- and small-scale initiatives in support of insurance business area
- Project management for transition of manual specimen processing to track-driven processing line directly to analysis units
- Point of contact for business partners with interfacing information systems
- Improved process flow of paper documents required for insurance applications

Hoechst Marion Roussel (pharmaceutical company)
1988 – 1998

Business Analyst, Hoechst Marion Roussel (pharmaceutical company)

1988 – 1998

- Business analyst supporting all financial systems
- IT lead for various large- and small-scale projects to improve productivity in the financial business area
- IT lead for implementation of SAP Accounts Payable Module

M&E Vendor Advisory Technical Architect – Jon Moreau

Jon Moreau's resume follows.

Jonathan Moreau

Director, Architecture

Jon Moreau is an experienced architect specializing in next-generation systems for both government and private sector clients. As a solution architect and enterprise architect, he brings extensive technical leadership and development experience. Jon has a solid foundation in enterprise architecture, cloud technologies, Agile frameworks such as Scrum and Kanban, as well as traditional software development processes. He excels in team management, technical leadership, and software implementation through all phases of a project lifecycle. Jon has a strong client focus, adept at building client relationships, gathering user stories, and providing recommendations. His business focus includes healthcare, government health and human services solutions, and HIPAA compliance. Jon is an excellent communicator with outstanding interpersonal, written, and verbal communication skills. He possesses the ability to motivate and guide teams to achieve solution goals. Additionally, Jon has multi-platform experience across various architectures and methodologies.

Professional Experience

Voyatek (formerly GCOM Software LLC, 3Sigma)
2019 – Current

Director of Nutrition Business Development

2020 – Current

- Move to a containerized architecture so developers can work in a way that is identical to production—Greatly reduced "works on my machine"-type bugs and allows devs to exercise the full range of functionality in the app when debugging locally.
- Incorporate all .NET code (.NET 6) to run on Alpine Linux containers, in dev (using Docker Compose) and in all deployed environments.
- Created full set of support libraries (logging, caching, business logic execution, auditing, message queueing, validation, e-mail/SMS, I/O, and HTTP) and moved to common code to NuGet packages for sharing across projects.
- Built an Azure DevOps pipeline integrated with Terraform for cloud deployments. This allows managing infrastructure as code and enabling quick implementation changes while enjoying the benefits of having changes in source control.

System Architect

2019 – 2020

Architect on transfer project for the Crossroads WIC system in North Carolina. Worked on software in the WIC space—desktop apps, web services (REST and legacy SOAP), and mobile applications using Xamarin iOS and Android. Focus was the modernization of legacy apps and moving towards shared architectural platform components that products can be built on.

Subject Matter Expertise

- Solution Architect
- Client and Business Focus
- Leadership
- Technology

Education

- DeVry University, BS, Telecommunications Management

Professional Certifications

- Azure Solutions Architect Expert
- Devop Engineer Expert

- Worked on a telehealth system for lactation consultants to connect with breastfeeding mothers using Xamarin Native and REST APIs built using Microsoft .NET.
- Provided system architecture expertise across multiple projects.
- Introduced automation to build and deployment processes, including the use of Octopus Deploy for deployment to internal and customer environments.

AMC Theatres

Mobile Application Architect

2017 – 2019

Worked on AMC's mobile application and the API that sits between it and the AMC platform API.

- Introduced new framework for mobile aggregation API to improve performance and scalability of the mobile application.
- Created a unified set of components that can be shared between the mobile application and aggregation API; including caching, configuration, HTTP, localization, logging, and business logic encapsulation. Having these components work identically in the mobile application and the API helps developers on the team switch more easily between the two codebases.
- iOS and Android mobile development using Xamarin native, with a focus on MVVM and message-based interaction between components.
- Created Xamarin bindings for several third-party components.
- Integrating the mobile app with backend systems for payments and fraud analysis.

Computer Sciences Corporation (CSC)

Advisor Application Designer

2015 – 2017

Worked on implementing good devops practices and building up the skills of the development team.

- Deployed a highly-available system on the Amazon Web Services (AWS) GovCloud platform, using SQL Server Always On Availability Groups, DFS, Active Directory, and auto-scaling.
- Developed a mobile application for iOS and Android (using Xamarin) and web portal (in Angular.js). Uses a REST API (built on Microsoft Web API) to provide payment processing for public welfare programs.
- Integrated Microsoft Azure multi-factor authentication with a Remote Desktop Gateway cluster deployed to AWS.
- Created a financial services platform for electronic benefit systems that integrates with WIC MIS systems.
- Worked to teach developers soft skills such as how to plan and estimate work or how to communicate with managers more effectively.
- Mentored developers on development concepts such as DI/IoC, functional decomposition, applying basic principles like SRP, how to write code that "fails fast," and how to design systems that can be easily deployed to a cloud environment.
- Provided technical support to sales teams as they try to earn new business.
- Introduced development teams to current tools and practices for continuous integration, then worked with those teams to add those tools to their existing workflow.
- Using current technologies to build, deploy, and maintain systems, including (among others): Visual Studio 2015, .NET 4.5, Angular, OAuth 2, Web API, SignalR, Twilio, ASP.NET MVC 5, SQL Server 2014, and Git
- Worked on tickets or helped to resolve complex production issues.
- Introduced a project management system (teamwork.com) to the management and development teams and helped them use it to improve planning and everyday work efficiency.

- Trained QA staff on continuous integration/devops to supplement those skills on the team.
- Completed complex interfaces between WIC MIS systems and external systems (such as Medicaid and USDA/FNS).
- Completed a subsystem that allows users to run a copy of the WIC MIS system when disconnected from the network, using SQL Server merge replication, and custom code.
- Conducted interviews for developer, architect, and software development manager positions.

Stonegate Mortgage
Senior .NET Developer
2014 – 2015

Worked on implementing good devops practices and building up the skills of the development team.

Created a prototype system to evaluate eligibility for jumbo mortgage loans. Worked with partner to gather requirements and define design. Responsible for implementing the designs.

- Created a front-end portal that communicated with a WCF services back end (for user data entry).
- Created a hybrid ASP.NET MVC 5 and SPA (single-page application) that used MVC for back-end support (such as bundling CSS and script files) and Knockout with JSON for the single-page functionality.
- Created a Web API infrastructure for authentication/authorization (using tokens) and application API access, to be used with an Angular front end.
- To decouple application components and provide separation of cross-cutting concerns used dependency injection and method interception.
- Implemented a novel algorithm for evaluating eligibility that did not use a traditional business rules engine.

Computer Sciences Corporation (CSC)
Systems Architect Principal Leader
2012 – 2014

Primarily worked on the Crossroads system, a service-oriented application with a WPF Windows client. Consulted as an architect on a wide variety of other projects.

- Created a load and performance test approach that worked within the unique technical constraints of a distributed client/server application. The application was services-based, but used an uncommon binding (Microsoft's binary-encoded SOAP) and had a custom message security structure. Created a few custom tools to help with the workflow for capturing traffic and parameterizing it for load testing.
- Helped development interpret performance test results to identify "heavy hitters"—areas of change that would have the most substantial impact on overall performance. Much of this work was in conjunction with .NET performance tools like ANTS Performance Profiler.
- Prepared the system for deployment to production. The production environments included fault-tolerant design features like clustered database servers, load-balanced application servers, and reverse proxy servers. Responsible for architecting necessary changes in the application and for directing the setup of CSC test lab components to mimic production since the development staff didn't have much experience with any of these technologies. This included Big-IP load balancers, web servers using IIS's Application Request Routing (reverse proxy), and application servers. After the lab environments were configured, the deployment process was updated to fit production deployment environments better.
- Replaced in-house database synchronization architecture used by occasionally connected clients with SQL Server merge replication. This allowed initial database download, schema changes, and data partitioning (segmenting the data each client receives) to be part of the sync process, managed by SQL Server.

- Worked closely with development to identify and fix architectural problems in areas like application security, web service usage, system performance, logging, and exception handling.
- Implemented a project to provide a public API and portal site (using ASP.NET MVC 5) for an industrial chemical company. Educated developers new to C# to help teams bridge the gap between VB.NET and C#.
- Introduced CI practices to development teams which had no previous exposure to automated builds, unit and regression testing, and gated releases driven by the CI tool (Atlassian Bamboo in this case).
- Worked with business unit managers to develop architectural plans & roadmaps for future development.
- Interviewed potential developer candidates.