North Carolina Department of Health and Human Services
2001 Mail Service Center • Raleigh, North Carolina 27699-2001
Tel: 919-733-4534 • Fax: 919-715-4645

Beverly Eaves Perdue, Governor

Lanier M. Cansler, Secretary

October 30, 2009

MEMORANDUM

TO: Division and Office Directors

FROM: Lanier M. Cansler

SUBJECT: Inadequate User Access Controls

Background

Pursuant to North Carolina General Statute (N.C.G.S.) § 159-34, the North Carolina Office of State Auditor (State Auditor's Office) submits the Single Audit Report to the Governor and General Assembly on a annual basis. The audit is conducted in accordance with the Government Auditing Standards issued by the Comptroller General of the United Sates, the requirements of the Single Audit Act Amendments of 1996, and the provisions of the Office of Management and Budget Circular A-133, entitled "*Audits of States, Local Government, and Non-Profit Organizations.*"

Issue

In previous Single Audit Reports, the State Auditor's Office has repeatedly issued DHHS audit findings for "**Inadequate Control Over User Access**." As you are aware, improper access to computer systems and systems applications can result in serious intentional or unintentional security breaches that place the confidentiality and integrity of our information systems at risk. In addition, the Statewide Information Technology Policies and Standards and DHHS Security Policies and Standards both require that DHHS control access to its system applications and conduct periodic, documented reviews of its users' access rights.

The State Auditor's Office and DHHS management are concerned about our repeated audit findings. As such, all DHHS divisions and offices will immediately implement the necessary procedures for deleting/revoking the access of its users in a timely manner.

Corrective Action

First and foremost, it is the duty of **supervisors** to inform IT security officials of all subordinate employee terminations or transfers **on or before the terminations/transfers**

take place. That is, no employee should continue to have access to a system after their work responsibilities have been terminated for the system. Just as we expect an employee to turn in their office keys on or before their last day at work, we fully expect access rights to our various systems to be terminated on or before their last day of work. The Department can not and will not tolerate laxity in this high risk area. **Failure to terminate system access in a timely manner by the supervisor as indicated above may result in disciplinary action, up to and including dismissal.** It is incumbent for each Division/Office to establish protocols to ensure compliance with this policy.

I have instructed the DHHS Privacy and Security Office to create various audit log reports so that the divisions and offices can audit themselves on a **monthly** basis to ensure that its employees have complied with granting and terminating appropriate employee system access. Once the divisions and offices have verified the audit log reports and taken appropriate action as necessary, they are to provide the monthly updated audit log reports to the DHHS Privacy and Security Office.

If you have any questions regarding the implementation of this policy, you may contact Pyreddy Reddy at 919-855-3090 or Dan Stewart at 919-733-4534.

cc: Pyreddy Reddy
Dan Stewart
Karen Tomczak
Allen Feezor
Maria Spaulding
Michael Watson
Emery Milliken
Security Workgroup Members