UNITED STATES DEPARTMENT OF EDUCATION
OFFICE OF INSPECTOR GENERAL

Information Technology Audits and Computer Crime Investigations

DATE: September 24, 2010

TO: Tony Miller
Deputy Secretary

William J. Taggart
Chief Operating Officer
Federal Student Aid

FROM: Charles E. Coe Jr. /s/
Assistant Inspector General
Information Technology Audits and Computer Crime Investigations

SUBJECT: Investigative Program Advisory Report
Weaknesses in the Process for Handling Compromised Privileged Accounts
(09-220005) Control No. L21K0002

The Office of Inspector General (OIG) conducted an investigative project from February 1 to June 30, 2010, to determine whether compromised privileged accounts were used by unauthorized individuals and to evaluate the Department's process for handling compromised privileged accounts. During this project, OIG found that:

- FSA does not identify all individuals whose data were potentially compromised
- The Department and FSA failed to conduct adequate log reviews of compromised privileged accounts to identify unauthorized activity.
- FSA keeps inadequate records of its remediation efforts for compromised privileged accounts.
- Two-factor authentication has not yet been required for remote access to Department and FSA systems.

To ensure that compromised privileged Department and FSA accounts are properly identified and analyzed and to prevent unauthorized access to Department systems, we made four recommendations:

1. Identify all potentially compromised PII by analyzing all account activity during the period that the privileged account was compromised.
2. Revise current methodology used to identify suspicious activity that indicates unauthorized access into privileged accounts. Log reviews of account activity should include, at a minimum, an analysis of originating IP addresses, login times, and amount of activity. If suspicious activity is identified, the user should be contacted to determine whether the user was responsible for the activity. Suspected unauthorized access to

government systems should be immediately reported in accordance with Handbook OCIO-14, "Handbook for Information Security Incident Response and Reporting Procedures."

3. Track compromised accounts and PII and the date of compromise, account deactivations, owner/borrower notifications, and the date and results of the account log review.
4. As recommended by OMB Memorandum M-06-16, implement two-factor authentication on any system where a user can log into a privileged account from the Internet, with an emphasis placed on financial systems and systems containing large volumes of PII.

Attached is the subject Investigative Program Advisory Report (IPAR) that covers our review of Weaknesses in the Process for Handling Compromised Privileged Accounts.

Corrective actions proposed (resolution phase) and implemented by your office will be monitored and tracked in the Audit Accountability and Resolution Tracking System (AARTS). The Office of the Chief Information Officer will be responding on behalf of the Office of the Deputy Secretary. ED policy requires that you develop a final corrective action plan (CAP) for our review in the automated system within 45 days of the issuance of this report. The CAP should set forth the specific action items, and targeted completion dates, necessary to implement final corrective actions on the findings and recommendations contained in this IPAR.

If you have any questions concerning this IPAR, please contact Special Agent in Charge, Mark A. Smith at (202) 245-7019.

Attachment

cc: Danny Harris, Chief Information Officer (CIO)
Richard Gordon, CIO, FSA
Charles Rose, General Counsel
Phillip Loranger, Chief Information Security Officer
Robert Ingwalson, Computer Security Officer, FSA