REDACTED

Incident Handling and Privacy Act Controls over External Web Sites

FINAL AUDIT REPORT

ED-OIG/A11I0006

June 10, 2009

Our mission is to promote the efficiency, effectiveness, and integrity of the Department's programs and operations.

U.S. Department of Education
Office of Inspector General
Information Technology
Audits Division
Washington, D.C.

NOTICE

Statements that managerial practices need improvements, as well as other conclusions and recommendations in this report represent the opinions of the Office of Inspector General. Determinations of corrective action to be taken will be made by the appropriate Department of Education officials.

UNITED STATES DEPARTMENT OF EDUCATION
OFFICE OF INSPECTOR GENERAL

Information Technology
Audit Division

June 10, 2009

Memorandum

TO: Margot M. Rogers
Chief of Staff

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

SUBJECT: Final Audit Report
Incident Handling and Privacy Act Controls over External Web Sites
Control Number ED-OIG/A11I0006

Attached is the subject final audit report that consolidates the results of our review of IT Security Controls over the Incident Handling and Privacy Act Controls over External Web Sites, A11I0006. An electronic copy has been provided to your Audit Liaison Officer(s). We received your comments concurring with the findings and recommendations in our draft report.

Corrective actions proposed (resolution phase) and implemented (closure phase) by your office(s) will be monitored and tracked through the Department's Audit Accountability and Resolution Tracking System (AARTS). ED policy requires that you develop a final corrective action plan (CAP) for our review in the automated system within 30 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 final audit report.

In accordance with the Inspector General Act of 1978, as amended, the Office of Inspector General is required to report to Congress twice a year on the audits that remain unresolved after six months from the date of issuance.

Because we identified vulnerabilities, weaknesses, and exposure to exploitation on the external infrastructure in network devices, servers, desktops, web applications, and databases, disclosure of the redacted information could harm the security posture of the Department. This report is exempt from public release pursuant to the Freedom of Information Act (FOIA); however this summarized version is made publicly available. The redacted portions of this report do not affect the validity of this report or management's response.

We appreciate the cooperation given us during this review. If you have any questions, please call [redacted].

Enclosures

cc: Danny Harris, Chief Information Officer
John Fare, Chief Information Officer, Federal Student Aid
Deborah Coleman, Audit Liaison for OCIO
Marge White, Audit Liaison for FSA
Dianne Novick, Office of Management, Privacy Advocate
Phillip Loranger, Chief Information Security Officer/Acting Director Information Assurance Services

TABLE OF CONTENTS

Page

Commonly Used Acronyms/Terms in this Report

CCU	Computer Crime Unit
CIO	Chief Information Officer
CSO	Computer Security Officer
Department	Department of Education
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DOB	Date of Birth
ED	U.S. Department of Education
EDCIRC	Education Computer Incident Response Capability
FOIA	Freedom of Information Act
FSA	Federal Student Aid
FISMA	Federal Information Security Management Act
GSA	General Services Administration
ID	Identification
IDPS	Intrusion Detection and Prevention System
IDS	Intrusion Detection System
IP	Internet Protocol
IT	Information Technology
NAEP	National Assessment of Educational Progress
NIST	National Institute of Standards and Technology
nslookup	Name Server Lookup
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
RDBMS	Relational Data Base Management System
SQL	Structured Query Language
SSN	Social Security Number
SSO	System Security Officer
URL	Uniform Resource Locator
US-CERT	United States Computer Emergency Readiness Team

EXECUTIVE SUMMARY

The Office of Inspector General (OIG) performed a review of the Department of Education's (Department) external web sites. This audit was conducted in accordance with the Federal Information Security Management Act (FISMA) as enacted by Title III of the E-Government Act of 2002, Public Law 107-347, and the Privacy Act of 1974. Specifically, we assessed whether information technology (IT) security controls were in place to protect Department resources in the areas of incident handling, security awareness and training, and Privacy Act compliance. FISMA requires the OIG to perform independent evaluations and testing of the effectiveness of information security control techniques and to provide an assessment of the Department's compliance**.**

Based on our review, the Department's Chief Information Officer (CIO) must improve security controls over the incident response and handling program and accelerate two-factor authentication for protecting Privacy Act information to adequately protect the confidentiality, integrity, and availability of the personally identifiable information (PII) data residing on public web sites. During our audit, we also identified significant conditions related to the work performed regarding [redacted] and public domain web site establishment and maintenance.

Incident Handling

- The Department did not have an effective incident response and handling program**.** The Department's CIO: (a) did not provide sufficient security awareness to Department users regarding [redacted]; (b) provided conflicting guidance regarding incident response reporting procedures; and (c) did not properly oversee the Department's Customer Service staff. The Department has a responsibility to implement all precautions to protect all vital PII data residing on the Department's network. Compromise of this data would cause substantial harm and embarrassment to the Department and may lead to identity theft or other fraudulent use of the information.

Two-Factor Authentication

- The Department's CIO did not implement two-factor authentication or other effective compensating controls commensurate with the risk and magnitude of harm resulting from a Department data compromise. Specifically, using information from two public web sites, we were able to use [redacted] techniques to remotely obtain access to sensitive Department information and PII. If sensitive Department information and PII data are compromised, the Department could suffer substantial embarrassment and that compromise may lead to fraudulent misuse of the information.

[redacted] Configuration

- The Department did not configure the [redacted]. Our tests demonstrated that unauthorized access to the system through [redacted] attacks could provide a potential malicious attacker with the capability of exploiting systems, deleting and/or modifying sensitive data, and causing serious harm to Department information. Users with malicious intent could gain access to the [redacted] for email spoofing, social engineering, and other possible malicious attacks.

Public Domain Web Sites

- The Department did not properly establish and maintain public domain web sites. Specifically, the Department did not: (a) properly track, update, and verify a directory of public web sites; (b) properly control internet protocol address assignment; (c) properly issue and administer web site certificates; (d) properly monitor public domain web sites; and (e) use approved domain names. The Department's CIO has the overall responsibility to implement all precautions to protect Department data residing on public domain web sites. Additionally, the public has the right to assume that web sites hosted or provided by the Department are valid and trusted. It is essential that the Department validate its public web sites and adequately protect the confidentiality, integrity, and availability of the PII data residing on public web sites.

In response to our draft report, the Department thanked the OIG for the opportunity to provide comments for this audit report. The Department also stated it concurred, as of the start date of this audit, with the findings and recommendations identified. In response to our system security review, management stated that corrective action plans for the weaknesses will be finalized through the Department's normal audit resolution process. [redacted].