UNITED STATES DEPARTMENT OF EDUCATION
OFFICE OF INSPECTOR GENERAL

Information Technology Audits and Computer Crime Investigations

DATE: July 18, 2011

TO: Danny Harris
Chief Information Officer

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

SUBJECT: Investigative Program Advisory Report
Incident Response and Reporting Procedures
(10-110283) Control Number L21L0001

The Office of Inspector General (OIG) has conducted investigations of potential computer crimes over the past two years. During these investigations, OIG has identified problems with how the U.S. Department of Education (Department) handled computer security incidents. Specifically, the Department did not detect, report, or respond to incidents in accordance with the Department's *Handbook for Information Security Incident Response and Reporting Procedures,* OCIO-14.

To ensure the Department's systems and networks are protected, OIG made one recommendation:

1. Enforce the contract's requirement for Perot Systems to comply with OCIO-14 when performing incident response, or develop a separate capability to perform incident response in accordance with OCIO-14. The incident response capability, whether or not maintained by Perot Systems, should include:

    - Providing incident response personnel with the appropriate training and tools to collect and preserve evidence in a quick and forensically sound manner (in person or remotely);
    - Analyzing information to determine the root cause of an incident and to determine the extent of damage;
    - Implementing appropriate hardware, software, and procedures to activate full content network monitoring in a timely manner to support the incident response process and to assist in discovery of the incident's root cause.

Attached is the subject Investigative Program Advisory Report (IPAR) that covers our review of the Incident Response and Reporting Procedures.

Corrective actions proposed (resolution phase) and implemented by your staff will be monitored and tracked in the Audit Accountability and Resolution Tracking System (AARTS). Department 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 recommendation contained in the IPAR.

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

Attachment

UNITED STATES
DEPARTMENT OF EDUCATION
OFFICE OF INSPECTOR GENERAL

Investigative Program Advisory Report

Incident Response and Reporting Procedures (10-110283)

Control Number: L21L0001

July 14, 2011

Table of Contents

Acronyms/Abbreviations Used in this Report

CIO	Chief Information Officer
CSMC	Cyber Security Management Center
Department	U.S. Department of Education
EDCIRC	U.S. Department of Education's Computer Incident Response Capability
EDUCATE	Education Department Utility for Communications, Applications and Technology Environment
IT	Information Technology
MSSP	Managed Security Services Provider
NetBIOS	Network Basic Input/Output System
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OCIO-14	Handbook for Information Security Incident Response and Reporting Procedures
OCIO-IA	Office of the Chief Information Officer, Information Assurance Services
OIG	Office of Inspector General
SER	Suspicious Event Report
SLA	Service Level Agreements
US-CERT	United States Computer Emergency Readiness Team

Investigative Program Advisory Report

Incident Response and Reporting Procedures

A. Executive Summary

During Office of Inspector General (OIG) investigations of potential computer crimes over the past two years, OIG identified problems with how the U.S. Department of Education (Department) handled computer security incidents. Specifically, the Department did not detect, report, or respond to incidents in accordance with the Department's *Handbook for Information Security Incident Response and Reporting Procedures,* OCIO-14, which is based on Federal guidelines and industry best practices.

OIG reported these issues to the Department starting in March 2009 (Attachment 1). These failures have prevented the collection of information that could aid the Department in identifying all compromised computers, the actions or vulnerability that enabled the incident, the objective of the incident, and the source. They have left the Department's systems and data vulnerable. In this report, we articulate our concerns and make a recommendation to address these problems.

B. Background

The Department's Chief Information Officer (CIO) is responsible for developing and enforcing the policy and procedures for information technology (IT) security within the entire Department. One aspect of IT security is the monitoring and detection of security incidents on a computer or computer network and properly responding to those incidents. OCIO-14[1] contains Department requirements related to incident response and reporting procedures.

OCIO-14 defines a computer security incident as "a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices."[2] Pursuant to OCIO-14, Office of the Chief Information Officer (OCIO) Information Assurance Services (OCIO-IA) manages the Department's Computer Incident Response Capability (EDCIRC), which serves as the primary Department-wide contact for all incident reporting and response activities. The EDCIRC coordinator is responsible for analyzing each incident and coordinating the response and additional reporting activities, to include the reporting of critical incidents to the United States Computer Emergency Readiness Team (US-CERT).[3]

Under OCIO-14, OIG performs investigations in response to attacks against, as well as the unauthorized access of, Department information systems, networks, databases, and computer communication systems. OCIO-14 also states it is necessary for any incident responder to

[1] OCIO-14 dated June 26, 2007, was updated on March 2, 2011. Unless otherwise specified, both versions of OCIO-14 are substantially similar for the issues addressed in this Investigative Program Advisory Report.
[2] OCIO-14 adopted the definition of the National Institute of Standards and Technology (NIST). NIST Special Publication 800-61: Computer Incident and Security Handling Guide, Revision 1 (March 2008).
[3] US-CERT is the Federal Incident Management Center for the Federal Government and serves as the focal point for cyber-security issues in the United States.

coordinate his or her actions with EDCIRC prior to taking any actions that may affect the data on a system. EDCIRC is directed to consult with OIG on appropriate actions to ensure that all potential evidence is preserved.

The EDUCATE Contract

The "Education Department Utility for Communications, Applications, and Technology Environment" (EDUCATE) contract between the Department and Perot Systems established a contractor-owner, contractor-operated IT service model for the Department under which the contractor is required to provide the total IT platform and infrastructure to support Department employees in meeting the Department's mission.

EDUCATE's Performance Work Statement, 6.1.1.6 – Security & Privacy Information Assurance, states in pertinent part,

> The contactor shall protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. The contractor shall provide comprehensive and all-inclusive security and privacy operations for EDUCATE IT Resources and services on a 24/7/365 basis. The contractor shall provide all necessary IT Resources to deliver all security and privacy operations herein. These services shall include all security and privacy operations in accordance with all Federal authorities (laws, regulations), Federal standards and guidelines, and Government and Department Policy (please refer to the Constraints section).

The referenced Constraints section states in pertinent part,

> The contractor's proposed solution shall be compliant, in all respects, with all applicable federal and departmental security, acquisition, IG, and asset management laws, regulations, rules, and policies. As new laws, regulations, guidance and policy is [sic] promulgated, the contractor is expected to review, plan for and comply with such authorities. The contractor shall comply with the following authorities included in, but not limited to, Sections 8.1 through 8.8.
>
> At section 8.8.8, included among listed Department of Education Policies, is the "Handbook for Information Security Incident Response and Reporting Procedures" (OCIO-14).

To clarify these security operations, the EDUCATE contract has Service Level Agreements (SLAs), which provide and describe the performance metrics needed to accomplish the intended mission. The SLAs covering Security Operations and Incident Response require the contractor to provide security operational services as determined by mutually agreed upon procedures, in accordance with US-CERT Federal Incident Reporting guidelines as defined at the time of the SLA's approval, and in accordance with the Infrastructure Solutions Security Operations Center Standard Operation Procedure (SOC SOP).

In August 2008, the Department acquired the independent services of the Cyber Security Management Center (CSMC) through an interagency agreement with the U.S. Department of Transportation.[4] This agreement states the objective is to "provide continuous monitoring and testing to ensure the EDUCATE contractor(s) delivers real-time detection, assessment, response and remediation related to all relevant cyber incidents." All incidents detected by CSMC are forwarded to EDCIRC. As set forth in OIG's Final Alert Memorandum, Implementation of the Managed Security Services Provider Contract, Control Number ED-OIG/L19K0011, dated September 24, 2010, (b) (7)(E)

To provide additional monitoring, the Department signed an interagency agreement with US-CERT to monitor the EDUCATE network with the Einstein program. The Einstein program monitors the network gateways of the participating agencies for unauthorized traffic. Thus, it provides the Federal civilian government with a process for collecting, correlating, analyzing, and sharing computer security information. The Einstein program is not meant to replace an agency's own security filtering or intrusion-detection systems, but it does provide US-CERT with the intelligence to see activity in various parts of the Federal networks and to alert on suspicious traffic if it is identified. US-CERT sends suspicious traffic information concerning the EDUCATE network to EDCIRC for additional investigation. (b) (7)(E)

(b) (7)(E)

C. The Department has not Detected, Reported, or Responded Appropriately to Security Incidents

Under OCIO-14 and applicable procedures, once a computer security incident is discovered, a number of actions are required (Attachment 2). The incident must be reported and evidence of the incident must be properly collected and reviewed (the detection/identification phase); the incident must be stopped before it spreads or causes more damage, the actions performed must be documented, and the destruction of evidence must be prevented (the containment phase); the cause of the incident must be identified and mitigated (the eradication phase); the affected systems must be restored to an unaffected state (the recovery phase); and the data and process must be reviewed to determine if there are any lessons learned (the follow-up phase). A root cause analysis (RCA) must be also be performed.[5]

[4] The interagency agreement was renegotiated on August 13, 2010.

[5] SLA SP-1 was the primary SLA applicable to the incident response process, and prior to its March 2011 revision, explicitly referenced an RCA. The current SLAs incorporate the SOC SOP which requires an RCA. OCIO-14, dated 03/02/2011, requires a root cause analysis to be performed as part of the final stage in the incident response life cycle. The previous version of OCIO-14, dated 06/26/2007, did not specifically state a root cause analysis was

Prompt notifications, the initial response, and access to data pertaining to the incident are all critical to ensuring that evidence is preserved, that the incident can be properly contained and mitigated, and that an accurate root cause analysis can be conducted. The following examples illustrate security incidents in Department systems that were not handled in accordance with OCIO-14 and applicable procedures. In particular, there were instances in the last two years when untimely notification, improper response, and lack of access to systems and data have resulted in the loss of potential evidence.

Malware Infection of EDUCATE Systems

In July 2010, a suspicious event report (SER) generated by Perot Systems indicated an EDUCATE computer, located in Washington, D.C., was communicating to suspected hostile websites, and the communication resembled known malicious traffic. Instead of capturing and preserving the evidence, which includes the network traffic, the live system data,[6] or a forensic image of the system, Perot Systems pulled the system off the network, thus preventing the collection of additional data that would have aided in discovering the root cause of the incident.

If Perot Systems had coordinated with EDCIRC, EDCIRC could have either collected the live data itself or contacted OIG to collect the data. A subsequent OIG review of the system determined the system was infected with malware, but OIG was unable to continue its investigation. OIG did not have enough data to determine the source or purpose of the infection, because Perot had unintentionally manipulated the data as a result of its failure to properly implement evidence collection procedures.

Similarly, a month later, a scheduled antivirus scan discovered malware on a different EDUCATE computer located in Washington, D.C. Again, instead of preserving the evidence, Perot Systems removed the system from the network and powered off the computer. As a result of Perot Systems' improper remediation, OIG was unable to obtain any live system data or an image of the system for analysis. Subsequent analysis determined the malware caused the computer to conduct unauthorized network scanning of the EDUCATE network. This malware technique is used to gather intelligence about the network and then to use that knowledge to successfully carry out additional attacks. Because Perot Systems did not respond properly to this incident, data was lost, and OIG was unable to determine the source and purpose of the scanning and how the system was initially infected.

EDUCATE Connections to a Known Malicious Website

One of the more serious recent incidents of improper response occurred on an internal system in the EDUCATE infrastructure located in the Plano Technology Center, (b) (7)(E) [redacted]. On July 6, 2010, EDCIRC and OIG received a SER from CSMC stating a computer

required, but it did require the incident to be documented and that the lessons learned from the incident be discussed and reviewed.

[6] Live system data is collected while the system is running and includes volatile and nonvolatile data. Volatile data includes system random access memory and running processes. Nonvolatile data includes system data such as registry settings and local log files.

was making numerous attempts to connect to a known malicious overseas Internet Protocol address through the Network Basic Input/Output System (NetBIOS) protocol stack.[7]

Upon notification of the incident, OIG requested, through EDCIRC, to have the live data on the system preserved. Perot Systems looked at the previous month's firewall logs and discovered the suspicious activity was on-going throughout the previous month. Instead of preserving the evidence, Perot Systems conducted a full system anti-virus scan.[8] Perot Systems contacted the vendor of the system's main application and learned the NetBIOS protocol stack was not required for the application to operate. Perot Systems then deactivated the NetBIOS protocol stack, and as a result, the observed traffic stopped.

On July 8, 2010, after OIG was notified of Perot Systems' actions, it requested a forensic image of the system and, if that was not immediately possible, OIG reiterated its request for the system's live data. OIG suggested the use of its Live Response Program to collect this data since there were Perot Systems technicians who were trained in its use.[9] Five days after this request, EDCIRC informed OIG that Perot Systems refused to run the program. Ultimately, OIG contacted the Department's CIO for assistance, and the CIO ordered Perot Systems to allow OIG to run the tool and collect the data. The live data was collected from the system by an OIG employee on July 14, 2010.

As required by its contract, Perot Systems provided a root cause analysis to OCIO-IA on August 5, 2010, but it was rejected by OCIO-IA, because it did not identify the root cause and contained inaccurate statements. To date, OCIO-IA has not received another root cause analysis on this incident.

On August 9, 2010, OIG made another request for a forensic image of the system and requested the backups of the system as it existed before the incident, but it learned Perot Systems had not made backups of this system. On September 2, 2010, Perot Systems shipped a logical copy of the system to OIG (Perot Systems told OIG that it could not shut the system down; therefore, only a logical copy, as opposed to a forensic image, could be provided). Given that a logical copy provides only a limited amount of data, OIG was unable to examine crucial areas of the system.[10]

---

[7] NetBIOS allows applications on different computers to communicate within a local area network.

[8] The scan detected no malware. However, many malware in circulation today will drop additional malware or utilities onto a system. Depending on the release date of the malware it may not be immediately identifiable by the anti-virus software. The majority of anti-virus vendors have a lag time from the time of an infection to the release of a patch to remove the malware.

[9] (b) (7)(E) OIG developed a program to assist the responding technicians in the collection of the necessary data, OIG's Live Response Program. This program is a series of scripts and programs built for the purpose of acquiring system evidence in a consistent and simple manner. Initially, Perot Systems agreed to use the program, but it later declined when OIG attempted to schedule training for Help Desk personnel, indicating it would take too much time to run. The program takes approximately 15 minutes to run.

[10] A logical copy of a system provides only a partial view of the entire system. It does not capture critical files that are in use by the operating system, nor does it collect deleted files, file slack, and free space. Critical evidence is often located and available for examination only within a forensic image of a hard drive.

After it reviewed the logical copy, OIG asked to speak with the Perot Systems technicians who worked on this incident. Perot Systems, through EDCIRC, informed OIG that it would not be allowed to talk directly to the Perot Systems' technicians, and it would need to submit questions to Perot Systems' managers who would get the answers and provide them to OIG. Ultimately, OIG was able to interview the technicians after several days of coordinating with a Perot Systems' attorney.

On October 8, 2010, OIG asked EDCIRC to capture the current network traffic of the system. (b) (7)(E) erot Systems stated it would start the network capture anyway and allow it to run for a 24-hour period. Two days later, OIG was informed no data was captured because the official request was never entered into the incident tracking system. (b) (7)(E)

At every critical juncture, Perot Systems or OCIO failed to properly respond to the NetBIOS incident. Although Perot Systems' initial actions may have contained the incident, Perot Systems destroyed potential evidence by running a full system anti-virus scan and then shutting off the NetBIOS protocol stack. (b) (7)(E) Perot Systems or OCIO forced OIG to step in to undertake these activities. By its delays in then allowing OIG to retrieve the live data, as well as by its failure to provide a forensic image and its impeding of – albeit temporarily – OIG's access to Perot System technicians, Perot Systems also hampered evidence collection.

(b) (7)(E)

D. Conclusion

The Department and its contractor Perot Systems have not properly responded to computer security incidents in accordance with OCIO-14 and Perot Systems' contract. Perot Systems' preferred method for dealing with many of the reported incidents seems to be to remove the infected system from the network and attempt to clean the system by running a virus scan, before there is any attempt to collect the potential evidence. Not only does this practice violate the containment procedures set forth in OCIO-14, but it also hampers the investigative processes that is part of the detection/identification phase, and can destroy the potential of determining the root

cause that is part of the eradication phase of OCIO-14. In addition, Perot Systems was unable to (b) (7)(E) was slow to provide requested data and access to Perot Systems' employees, and has not completed root cause analyses that identified the root cause of these incidents.

Because Perot Systems has ignored the initial stages of the incident response life cycle and proceeded directly to the recovery phase, the Department has been unable to discover what it did not know about the incident, including the source of the problem and the various systems that might be impacted. The Department is unable then to determine if there are any lessons to be learned from the incident as is required in the follow-up phase of OCIO-14. This could leave the Department's data and systems vulnerable.

E. Recommendations

To ensure the Department's systems and networks are protected, OIG recommends the Chief Information Officer to:

Enforce the contract's requirement for Perot Systems to comply with OCIO-14 when performing incident response, or develop a separate capability to perform incident response in accordance with OCIO-14. The incident response capability, whether or not maintained by Perot Systems, should include:

Providing incident response personnel with the appropriate training and tools to collect and preserve evidence in a quick and forensically sound manner (in person or remotely);
Analyzing information to determine the root cause of an incident and to determine the extent of damage;
Implementing appropriate hardware, software, and procedures to activate full content network monitoring in a timely manner to support the incident response process and to assist in discovery of the incident's root cause.

Attachment 1 - Previous Findings

Over the last two years, OIG identified, reported, and made recommendations to the Department on the following weaknesses within incident response and reporting, based on OCIO-14 requirements:

Memorandum, OIG Information Technology Security Concerns, dated March 11, 2009.

- Department systems made frequent outbound connections to foreign sites known to contain malware.
- CSMC alerts increased as a result of improved coverage and tuning. CSMC started to generate repeat findings because the Department failed to identify the computer responsible for the suspicious activity in prior alerts.
- Since January 2009, there were approximately 60 virus or malware detections on Department computers per week.
- There was an increase in keylogger data incidents as reported by US-CERT.

Email to the OCIO-Information Assurance: Urgent IT Security Issue, dated June 8, 2010.

Based on a review of network traffic, OIG identified potentially compromised systems, as well as numerous Department computers, which were communicating with hostile Internet sites that had not yet been identified by the Department as suspicious.

Investigative Program Advisory Report, Bypassing of Web Content Filtering, Control Number L21K0001, dated July 20, 2010.

Users throughout the Department were circumventing web filtering by adding an "s" to the "http" before a uniform record locator in their browsers. The https traffic went undetected under the current configurations of the web filtering program.

(b) (7)(E) [redacted]

Final Alert Memorandum, Implementation of the Managed Security Services Provider Contract, Control Number ED-OIG/L19K0011, dated September 24, 2010.

The Department had not effectively implemented its managed security services provider (MSSP) contract with CSMC. The memorandum discussed (b) (7)(E) [redacted]

Attachment 2 - OCIO-14 Incident Response Life Cycle

Summarized below are six stages of the incident response life cycle, as found in OCIO-14, which adopted from NIST Special Publication 800-61, Revision 1:

Preparation: The initial phase consists of the development of policy and procedures and the identification and implementation of other components required for the response.

Detection/Identification: This phase involves the collection and review of the evidence of an intrusion.

Containment: This phase includes the stopping of an incident before it spreads or causes more damage, while also documenting the actions performed, performing two disk images of the system and the gathering, and reviewing the network, system and application logs.

Eradication: The identification and mitigation of the cause of the incident is the purpose of this phase.

Recovery: The restoration of affected systems to an unaffected state and their validation in terms of functionality and security are the components of this phase.

Follow-up: The final part of the incident response process involves the review of data, in an effort to determine if there are any lessons to be learned from an incident.

UNITED STATES DEPARTMENT OF EDUCATION

OFFICE OF THE CHIEF INFORMATION OFFICER

June 24, 2011

MEMORANDUM

TO: Charles E. Coe, Jr.
Assistant Inspector General

FROM: Danny A. Harris, PhD.
Chief Information Officer
Office of the Chief Information Officer

SUBJECT: Investigative Program Advisory Report (IPAR)
Control No. L21L0001

Thank you for the opportunity to respond to the Office of Inspector General's (OIG) Investigative Program Advisory Report (IPAR), "Incident Response and Reporting Procedures" (Case # 10-110283) Control No. L21L0001. OIG conducted an investigation over the past two years starting in 2009 that revealed instances in which the Department did not detect, report, or respond to incidents in accordance with the Department's *Handbook for Information Security Incident Response and Reporting Procedures,* OCIO-14. The report provides recommendations that the Chief Information Officer (CIO) take one action to improve incident response throughout the agency. Below is the Department's proposed response to your recommendation based upon the draft report:

Recommendation 1. Enforce the contract's requirement for Perot Systems to comply with OCIO-14 when performing incident response, or develop a separate capability to perform incident response in accordance with OCIO-14. The incident response capability, whether or not maintained by Perot Systems, should include:

- Providing incident response personnel with the appropriate training and tools to collect and preserve evidence in a quick and forensically sound manner (in person or remotely);
- Analyzing information to determine the root cause of an incident and to determine the extent of damage;
- Implementing appropriate hardware, software, and procedures to activate full content network monitoring in a timely manner to support the incident response process and to assist in discovery of the incident's root cause.

While we agree with this recommendation, we would like to state that the Office of the Chief Information Officer (OCIO) has been exercising due diligence in steadily improving the Department's Incident Response program. More specifically OCIO IAS has initiated and/or completed the following activities to ensure the Department and its contractor, Dell Systems (formerly known as "Perot Systems"), properly responds to computer security incidents in accordance with the Department's *Handbook for Information Security Incident Response and Reporting Procedures,* OCIO-14:

- OCIO IAS has recently hired a GS-15 Cyber Security Director to oversee the operational protection and defense of the Department's information and information systems. The U.S. Department of Education's Computer Incident Response Capability (EDCIRC) was given two additional staffing allocations from within IAS to include a certified computer forensic analyst.
- All EDCIRC personnel have attended specialized training in Incident Handling and Response and/or forensic analysis within 2011.
- OCIO IAS has strengthened the EDCIRC relationship with Cyber Security Management Center (CSMC), the Department's Federal Managed System Security Provider and built enhanced analysis capabilities to include analysis of advanced persistent threat activity. Furthermore, OCIO is working with CSMC to expand visibility of all Department networks (to include FSA and American Data Technology Incorporated-ADTI) by installing Network Intrusion Detection Systems (NIDS) on the inside of the firewalls within the networks. Additionally, both the EDCIRC and CSMC are leveraging and utilizing Einstein capabilities to conduct inbound and outbound traffic analysis.
- OCIO is leveraging the IA Enhancement funding, authorized by the Secretary, to develop an automated Enterprise-wide Continuous Monitoring program that enables the EDCIRC to have near-real time situation awareness of system configurations, vulnerabilities, automated change detection, and automated patch management. Additionally, the EDCIRC has purchased forensic analysis tools which will assist with discovering any root cause analysis for intrusions when they occur.
- OCIO is leveraging the IA Discovery Project, supported and endorsed by the Secretary, to identify all assets on the Education Department Utility for Communications, Applications and Technology Environment (EDUCATE) and the FSA Virtual Data Center (VDC) networks, identify and remediate associated vulnerabilities, and to establish recommendations and a roadmap to incorporate solutions to address identified systemic issues. This effort kicked-off in January 2011 and is nearing completion. Through this endeavor several critical vulnerabilities have already been identified and remediated.
- OCIO has also established new Security Service Level Agreements with Dell Systems in March 2011 to address identified weaknesses in the government's ability to track security issues. The Chief Information Security Officer (CISO) is continuing to review and analyze security requirements within the Dell Systems contract and how those requirements are being enforced.
- OCIO IAS has initiated an enterprise approach to information security working closely with Federal Student Aid (FSA), Institute of Education Sciences (IES), and other data

centers to consolidate and standardize capabilities, standardize processes, improve response times, and achieve cost efficiencies through economies of scale.

- OCIO-14, Handbook for Information Security Incident Handling and Reporting Procedures has been updated, staffed, and published in March 2011.

In summary, the OCIO acknowledges that the capabilities, processes, and procedures that have been or are being put into place are still nascent but feel that the Cyber Security Incident Response capability within the Department is being built on a strong foundation and has a solid trajectory for enhanced capability. The OCIO and the EDCIRC will continue to work with FSA, Dell Systems, and the OIG to synchronize and enhance our business processes to ensure the protection and defense of the Department of Education's information and information systems.

Thank you again for the opportunity to comment on this report. If you have any questions, please contact me at (202) 245-6252 or Danny.Harris@ed.gov.