**UNITED STATES DEPARTMENT OF EDUCATION**
**OFFICE OF INSPECTOR GENERAL**

THE INSPECTOR GENERAL

August 15, 2016

The Honorable Ron Johnson
Chairman, Committee on Homeland Security and Governmental Affairs
U.S. Senate
328 Hart Senate Office Building
Washington, D.C. 20510

The Honorable Thomas R. Carper
Ranking Member, Committee on Homeland Security and Governmental Affairs
U.S. Senate
513 Hart Senate Office Building
Washington, D.C. 20510

The Honorable Jason Chaffetz
Chairman, Oversight and Government Reform Committee
U.S. House of Representatives
2157 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Elijah Cummings
Ranking Member, Oversight and Government Reform Committee
U.S. House of Representatives
2471 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairmans Johnson and Chaffetz, and Ranking Members Carper and Cummings:

The Cybersecurity Act of 2015 established a reporting requirement for Inspectors General of agencies operating Federal computer systems that provide access to personally identifiable information. Specifically, we are required to report on the logical access controls, the information security management practices employed for these systems, and the policies and procedures that ensure that entities providing services are implementing the same information security practices. Enclosed with this letter you will find the results of our review.

If you have any questions or if you need any additional information, please do not hesitate to contact me directly at (202) 245-6900, or have a member of your staff contact our Congressional Liaison, Catherine Grant, at (202) 245-7023.

Sincerely,

Kathleen S. Tighe
Inspector General

Enclosure

cc: The Honorable John King, Secretary, U.S. Department of Education

# Office of Inspector General's Report on Policies and Practices for Covered Systems at the Department of Education
# August 15, 2016

The Cybersecurity Act of 2015 (Act), enacted December 18, 2015, as Division N of the Consolidated Appropriations Act, 2016, established a reporting requirement for Inspectors General whose agencies operate a covered system, defined as a national security system or a system that provides access to personally identifiable information. Specifically, we are required to report on the logical access controls, the information security management practices employed for these systems, and the policies and procedures that ensure that entities providing services are implementing the same information security practices.

Section 406(b) of the Act requires the Inspector General of each covered agency, not later than 240 days after the date of enactment, to submit to the appropriate committees of jurisdiction in the Senate and House of Representatives a report of information collected from the agency describing policies and practices in five specified areas. We list the five specified areas and provide the requested information below. We relied on information collected in work performed by Office of Inspector General (OIG) to report the requested information. Except as noted in the discussion below of the results of specified OIG audits under (A), we did not perform work to verify or validate the implementation of the described policies and practices, although many of the policies and procedures will be verified and validated through our Federal Information Security Modernization Act of 2014 (FISMA) work this year.

The policies and practices described below apply to all U.S. Department of Education's (Department) systems. This includes covered systems that provide access to personally identifiable information, as well as other systems. The Department does not operate a national security system.

## Department's Policies and Practices for Covered Systems

### (A) Description Of The Logical Access Policies And Practices Used By The Covered Agency To Access A Covered System, Including Whether Appropriate Standards Were Followed

The Department's Office of the Chief Information Officer (OCIO) established the Departmental Handbook OCIO-01, "Information Assurance/Cybersecurity Policy" (OCIO-01), dated August 2014, to provide policy regarding information assurance/cybersecurity for all information technology (IT) assets and services operated within or, on behalf of the Department. Specifically, for logical access, OCIO-01 requires proper identification and authentication for all users of government systems before allowing them access to Departmental systems. Further, it is the Department's policy to limit system access to authorized users, processes acting on behalf of authorized users, devices (including other systems), and to the types of transactions and functions that authorized users are permitted to exercise. The responsibility for implementation and enforcement rests jointly with the Program Offices (PO) that own the systems and data, and the Personnel Security office of the Office of Management (OM).

To supplement the OCIO-01 policy, the Department also established "Logical Access Control Guidance, Version 6.1," (LACG v6.1), issued in March 2013, to ensure that only authorized individuals gain access to information systems, are assigned minimum privileges to complete their tasks, and are individually accountable for their actions. The guidance also states that access to sensitive system resources will be controlled and limited based on positive identification and authentication mechanisms.

As part of our FISMA Report for Fiscal Year (FY) 2015, OIG found that the Department established policies and procedures for managing its identity and access management program for its employees that is consistent with National Institute of Standards and Technology standards. Specifically, we found that for the systems we reviewed (which included covered systems), the Department:

- established a mechanism for tracking and monitoring internal users;
- maintained and reviewed user activity logs;
- established a process tracking and monitoring employee adherence to rules of behavior for use of Department systems;
- enforced the 90-day password change requirement;
- granted user access to its systems and facilities in accordance with Federal guidance;
- required users, including contractors and third parties, to use two-factor authentication;
- established a process to ensure that employees were granted access based on needs and separation of duties principles; and
- established a process for the termination and deactivation of user access for employees when no longer required.

However, during our FY 2015, 2014, and 2013 FISMA audits, we also identified instances where appropriate standards were not always being followed. These instances are set forth below.

<u>The U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2015, issued on November 13, 2015 (ED-OIG/A11P0001)</u>

OIG found that Federal Student Aid's (FSA) implementation and management of the technical security architecture supporting the Department's mainframe environments needed improvements to effectively restrict unauthorized access to the Department's information and resources. Specifically, for the mainframe environments at the Virtual Data Center (VDC) and Total System Services, Inc. (the data center that houses the Common Origination and Disbursement (COD) system), we found accounts for authorized Departmental users with excessive permissions, unauthorized access to data, weak data resource rules, unclear security software privileges, account management weaknesses, and inadequate separation of duties. In addition, we found that FSA did not have reasonable assurance that commercial users of a subcontractor-operated mainframe supporting the COD system do not have access to Department data.

For the recommendation to correct vulnerabilities relating to the VDC mainframe environment, the Department identified in its Audit Accountability and Resolution Tracking System that corrective action plans were completed in March 2016. We will verify these corrective actions

during our next mainframe vulnerability assessment testing of the VDC environment. During our FY 2016 FISMA audit planning, we were informed that FSA is going to migrate its COD operations that were processed in a mainframe environment to a midrange environment.[1] We are reviewing this new processing environment as part of our FY 2016 FISMA vulnerability assessment and penetration testing of the COD system. Since COD will not be using mainframes for its processing, the findings that were identified in the FY 2015 FISMA report are no longer applicable.

The U.S. Department of Education's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2014, issued on November 12, 2014 (ED-OIG/A11O0001)

OIG audit work showed that the Department and FSA did not fully comply with the Identity and Access Management reporting metric. We reported that improvement was needed in (1) the overall identity and access management process; (2) password authentication; and (3) users' logical access controls. Specifically, we found that:

- OCIO had not fully established policies and procedures to (1) identify all devices that were attached to the network; (2) distinguish those devices from users; and (3) authenticate devices that were connected to the network.
- The Department did not consistently follow and enforce the required Federal and Departmental guidelines requiring users to update their network passwords.
- FSA did not fully establish effective access controls for a major system to ensure users of an application were not able to manipulate their user settings. Specifically, during penetration testing of this FSA system, the OIG's testing team was able to perform unauthorized actions by elevating the privileges of a basic user account.

As of September 2015, the Department reported that all corrective actions were completed to implement the three recommendations identified in the report. However, it should be pointed out that the first two bullets were repeat findings, originally identified in the FY 2011 and 2013 FISMA audits, where the Department reported they had completed the proposed corrective actions, and implemented the recommendations. We are validating these corrective actions as part of our FY 2016 FISMA reporting.

The U.S. Department of Education's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2013, issued on November 13, 2013 (ED-OIG/A11N0001)

OIG audit work showed that the Department did not fully comply with the Identity and Access Management reporting metric. We reported that improvement was needed in (1) the overall identity and access management process; (2) password authentication; and (3) the deactivation of users' accounts. Specifically, we found that:

[1] A midrange computer system features computers that have more processing power than personal computers, but are less powerful than mainframe models. These types of systems involve a broad range of memory capacity, processing power, and applications for business or scientific use.

- OCIO had not fully established policies and procedures to identify all devices that were attached to the network, distinguish those devices from users, and authenticate devices that were connected to the network.
- The Department did not consistently follow and enforce the required Federal and Departmental guidelines requiring users to update their network passwords. Although OCIO officials explained that the Department's Active Directory is configured to automatically notify and prompt users to change their network passwords after 90 days, our review showed that (1) about 1,200 of 9,523 users did not change their passwords for more than 90 days as required; (2) 165 users did not change their password for more than 600 days; and (3) 5 users were able to access the network despite expired passwords (3) user accounts had been expired for 2 years, and 2 user accounts for a year).
- The Department did not consistently and effectively ensure that user accounts inactive for 90 days were disabled, as required by Federal and Departmental guidelines. Specifically, we found that as of May 2013, 824 of the 896 inactive user accounts were not being disabled as required.

As of May 2014, the Department reported that all corrective actions were completed to implement the three recommendations identified in the report.

The aforementioned audit reports can be found in their entirety on our OIG website: http://www2.ed.gov/about/offices/list/oig/areports.html

**(B) Description And List Of The Logical Access Controls And Multi-Factor Authentication Used By The Covered Agency To Govern Access To Covered Systems By Privileged Users**

**Logical Access Controls**

LACG v6.1 defines position roles and responsibilities to ensure effective implementation and management of the guidance by establishing an access control structure and assigning security responsibilities for (1) the CIO; (2) the Chief Information Security Officer; (3) the Assistant Secretary for Management; (4) OM; (5) the Information System Security Manager; (6) Information System Security Officers (ISSO); (7) Network Security Officers; (8) Information System Owners; and (9) Users. LACG v6.1 further identifies logical access control areas, to include privileged users, described in detail below.

Access Enforcement

Access control policies (e.g., identity based policies, role-based polices, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) should be designed to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system. These policies should be configured to distinguish between users and devices connected to the network. For third party and custom written applications, to the greatest extent possible, technical security controls are utilized through operating systems or database management systems. System database administrators are required to configure

operating systems and databases to implement applicable password management requirements and enforce the Department's password standards. Accounts are also required to be configured to be disabled after 90 days of inactivity. All devices are required to receive Enterprise Architecture Review Board (EARB) approval before being connected to the Department's network. Further, devices must be authenticated consistent with FISMA and applicable regulations, statutes, and applicable Federal governance. Direct connections from public networks systems and databases, even to view data, is prohibited.

Information Flow Enforcement

POs are required to ensure that systems categorized in accordance with Federal Information Processing Standards Publication 199, "Standards for Security Categorization of Federal Information and Information Systems," as being a "Moderate" or "High" impact system control the flow of information within a system, and between interconnected systems. This control is accomplished by configuring network devices (such as firewalls and routers) to restrict protocols and ports to certain segments of the network and between specific devices. This control can also be accomplished through application design by forcing data to flow from designated point and prevents or minimizes the need for data to be removed from authorized repositories.

Separation of Duties

Each PO is required to establish appropriate divisions of responsibilities and separation of duties to eliminate conflicts of interest in the responsibilities and duties of individuals. Information systems shall also enforce separation of duties by limiting access authority.

Least Privilege

Departmental information system configurations are required to enforce the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) and information systems for the performance of specified tasks. LACG v6.1 specifically prohibits users from gaining administrator privileges without a validated business reason. Exceptions must be documented and approved by the ISSO and remain available for audit verification. Also, access to system utilities is approved by the ISSO, and limited to users and administrators with an approved need. Information system configurations must employ the concept of least privilege for specific duties (including specific ports, protocols, and services) in accordance with risk assessments to adequately mitigate risk to the Department's IT operations and assets. LACG v6.1 also recognizes that since user access privileges may change over time, it is imperative that reviews are conducted more frequently than on an annual basis. These reviews should ensure that user access privileges are current, and the privileges granted are authorized. Users should be granted only the most restrictive set of privileges needed to perform authorized tasks.

Unsuccessful Login Attempts

POs are required to follow OCIO-01 and the National Institute of Standards and Technology Special Publication 800-63, "Electronic Authentication Guidance," to ensure information

systems employ minimum difficulty standards for passwords and personal identification numbers. POs are also required to configure systems to limit the number of login attempts before locking user access, triggering an investigation as to the reason for the failed login attempts.

System User Notification

Upon initiation of a user's attempt to access a system, the system should provide an indication as to the nature and usage of the system. These specific requirements are found in the "Warning Banner" section of OCIO-01. Warning banner formats must be approved by the Department's Office of General Counsel.

Concurrent Session Control

POs are required to ensure concurrent user logins are not permitted without written approval from an ISSO or Authorizing Official.

Session Lock and Termination

LACG v6.1 requires that password protected screen savers be automatically activated on workstations after a maximum of 30 minutes of inactivity. The password used to unlock the screensaver is required to comply with Departmental password construction standards. Also, IT systems are required to be designed and configured to automatically terminate sessions after a specified period of inactivity.

Supervision and Review of Access Control

Whenever possible, automated tools should be used to identify all devices that are attached to the Department's network. Audit records (e.g., user activity logs) for systems categorized as "High" or "Moderate" impact, in accordance with Federal Information Processing Standards 199, are to be reviewed every 30 days, and "Low" impact systems every 60 days for inappropriate or suspicious activities. Users are required to report to the Information System Security Manager all devices that are found unidentifiable (labeled as "unknown") and network connectivity shall be terminated.

Remote Access

Remote access to Departmental information systems is available through virtual private network connections and multi-factor authentication is required.

Wireless Access Restrictions

Wireless transmission of Departmental information is only allowed by secured means and when approved through official Departmental channels. For wireless access, the use of Wide Area Network and Wide Local Area Network technology is permitted if (1) anti-virus software application code version and definitions are maintained; (2) access points are registered and

maintained by OCIO; (3) access points maintain record logs on unauthorized access attempts in accordance with security requirements (recording capabilities must be active at all times while access points are operational); and (4) Service Set Identified character strings do not reflect the name of the Department, Agencies, POs, office addresses, or other product information.

Access Control for Portable and Mobile Devices

Users can only connect government-issued wireless devices to the Department's network infrastructure, with OCIO having approval for the types of wireless devices that are deployed. Users with personally-owned mobile and wireless devices that want to connect to the network infrastructure for government business purposes must register the devices with the OCIO organization. Departmental issued wireless devices should (1) have approved anti-virus software installed and maintained; (2) have access controls that allow for passwords and personal identification number complexity in accordance with the Department's password standard which defines password configuration settings; (3) have a time-out capability that does not exceed 30 minutes; and (4) encrypt Department-sensitive data on wireless devices.

**Multi-Factor Authentication**

In January 2016, the Department established the "Mandatory Use of Personal Identity Verification (PIV) Cards" standard operating procedure that requires the mandatory use of two-factor authentication in accordance with Homeland Security Presidential Directive 12, "Policy for a Common Identification Standard for Federal Employees and Contractors," to ensure proper identification of all users having access to information and information systems. Specifically, the standard operating procedures requires that all Federal employees and contractors accessing the Department's network and/or information systems are required to use two-factor authentication. All users must have a PIV-enabled identification card and a personal identification number in order to access the Department's network and/or information systems. PIV cards are issued to employees by OM on the first day of processing, or prior to allowing any network access. OM also verifies that employees have completed the appropriate security awareness training, and that a security background investigation was completed prior to issuing the PIV Card. Contracting Officer's Representatives/Program Managers ensure the same process is conducted for all contractors requiring access to the network, prior to the issuance of a PIV card. The standard operating procedure further points out that allowing users to access/authenticate network assets and information systems with a single factor, username/password, or two-factor using something other than approved PIV credentials, is considered a risk and therefore must be treated as a weakness and documented as such.

Departmental Handbook OCIO-15, "Handbook for Protection of Sensitive but Unclassified Information", issued in March 2007, further emphasizes that the Department leverages the Homeland Security Presidential Directive 12 requirement to enforce the use of two-factor authentication for remote access to the Department's information resources.

### (C) If The Covered Agency Does Not Use Logical Access Controls Or Multi-Factor Authentication To Access A Covered System, A Description Of The Reasons For Not Using Such Logical Access Controls Or Multi-Factor Authentication

As described above under (B), the Department uses logical access controls and multi-factor authentication. According to the Department's "Mandatory Use of Personal Identity Verification Cards" standard operating procedure, although the use of PIV credentials is required for multi-factor authentication, OCIO acknowledges circumstances where it may be difficult to implement the requirement. The standard operating procedure identifies exceptions that are recognized when the use of a PIV card may be waived. However, the appropriate risk decisions associated with the PIV card waiver must be documented in a Risk Acceptance Form (RAF) and approved by the Department's Chief Information Security Officer prior to the user being granted access. Exceptions to using a PIV card are identified below.

User Forgot/Locked PIV Card

This exception occurs when an existing account or credential is temporarily unavailable or inaccessible. When this occurs, a one-time/one day exception is approved. If the user requires a second day, the user's immediate supervisor must request approval from the Chief Information Security Officer. If additional days are required, the user must report the card as lost to the Department's Security Operations Center (EDSOC) and OM Security Services. OM Security Services terminates the card and the EDSOC reports the lost card as a cyber security incident.

Enterprise Failure of PIV Infrastructure

This occurs when an unplanned failure (such as a disaster recovery or emergency situation occurs) of the IT infrastructure requires immediate access to network assets or information systems.

Technically Not Feasible

This occurs when PIV or supporting IT infrastructure prohibits a user from technically accessing network assets or information systems using a PIV card or credentials. The ISSO or system owner must submit a RAF for approval.

Mobile Devices

Currently, government furnished equipment and bring your own devices mobile devices do not support the PIV card/credentials. The ISSO or system owner for the Department's general support system submits and maintains the enterprise level RAF for the government furnished equipment and incorporates a RAF requirement as part of the bring your own devices process.

Shared IT Asset

A shared IT asset is one that is shared by two or more individuals. Due to the asset-based PIV implementation at the Department, an asset designed as PIV exempt applies to all users

accessing the asset and therefore, the shared asset owner must submit a RAF. The following shared asset exceptions are approved until January 2017: (1) kiosks; (2) regional training facilities; (3) video teleconference centers; (4) OM security guard stations; and (5) assets that are part of the Department's loaner pool. Any changes or continued exceptions beyond January 2017 require a RAF approved by the Chief Information Security Officer or designee.

**(D) Description Of The Following Information Security Management Practices Used By The Covered Agency Regarding Covered Systems:**

**(i) The policies and procedures followed to conduct inventories of the software present on the covered systems of the covered agency and the licenses associated with such software**

Departmental Directive OCIO 3-110, "Software Asset Management and Acquisition (SAMA) Policy" (OCIO 3-110) was issued in March 2015 in response to compliance standards, applicable laws, and licensing restrictions as outlined by Executive Order 13103, "Computer Software Piracy." The Directive applies to all Departmental employees and contractors utilizing Department-owned IT equipment and software, and all IT equipment that is connected to the Department's network. OCIO 3-110 requires that the OCIO IT Program Services (ITPS) and the IT Principal Office Coordinator (POC) conducts an annual assessment of software management procedures, practices and an inventory of installed software and related license agreements, purchase invoices, and other documentation showing evidence of licensed software that is currently in use. OCIO ITPS and the IT POCs use a software asset management tool to retrieve reports to assist with enforcing and validating OCIO 3-110 policy.

All EARB approved software is available to Department employees for use (e.g., installation or re-installation, replacement, and upgrades) with approval from their IT POC or designee (providing that licenses are available). For software that the Department or employees has legally obtained licensing and approval, OCIO ITPS maintains a software library for the Department for original software licenses, certificates of authenticity, purchase invoices, completed registration cards, original software media (e.g., diskettes or CD-ROMs), user, administrator, and assessment information. IT POCS are required to enter all applicable information in the software asset management tool, with OCIO ITPS acting as system administrator for the tool.

**(ii) What capabilities the covered agency utilizes to monitor and detect exfiltration and other threats, including:**

**(I) Data loss prevention capabilities**

As part of the Department's ongoing Cybersecurity initiatives, the OCIO's Information Assurance Services is in the process of establishing a Data Loss Prevention (DLP) system designed to protect personally identifiable information in the Department's network by providing technical capabilities to detect, prevent, and report the leakage of personally identifiable information data (unencrypted sensitive data such as social security numbers (SSNs) and financial information) in email and web traffic that leaves the Department's network boundary.

However, the tool used to monitor DLP does not monitor encrypted emails that remain within the Department's network. The Department's DLP system is also designed to reduce the likelihood of unintentional or inadvertent actions that leak data and cause security incidents. However, as of July 2016, due to technical issues, the implementation of the DLP blocking feature has been postponed. As an additional protection, the Department advised its employees to use the WinZip program to encrypt personally identifiable information prior to emailing outside the Department's network. The transmission of unencrypted personally identifiable information is considered a security violation that must be reported and handled in accordance with the Department's incident handling procedures.

### (II) Forensics and visibility capabilities

Departmental Handbook OCIO-14, "Handbook for Information Security Incident Response and Reporting Procedures" (OCIO-14), dated March 2011, provides incident response and reporting procedures to ensure appropriate and expeditious handling of information security incidents that may affect the Department's normal business operations. The handbook also contains a chain of custody form to be used during incident handling.

OCIO's Information Assurance Services office manages the Department's Computer Incident Response Capability (EDCIRC). The EDCIRC Coordinator serves as the primary focal point for Department-wide incident reporting and escalation activities. EDCIRC coordinates with OIG on matters that relate to potential criminal violations, or other matters within OIG's jurisdiction related to computer incidents. The OIG component responsible for investigating computer security incidents is the Technology Crimes Division (TCD), which falls under the Assistant Inspector General for IT Audits, and Computer Crime Investigations. TCD performs cyber-criminal investigations in response to attacks against, as well as unauthorized access of, the Department's information systems networks, databases, and computer communications systems. It also investigates the criminal misuse of Departmental computers and performs forensic analysis of computer media in support of criminal investigations. TCD consists of special agents with a formal technical background and all computer crime investigators have full statutory law enforcement authority as granted by Congress.

OCIO-14 emphasizes that TCD cannot investigate a computer security incident without receiving a timely incident report. Thus, failure to provide OIG timely incident reports may directly impede the criminal investigative activities of the TCD staff. If incidents are not reported as soon as possible, the Department may lose information that is vital to the securing of evidence, as well as making important connections to ongoing cases and making decisions about initiating new cases.

### (III) Digital rights management capabilities

Departmental Directive OCIO 3-110, "Software Asset Management and Acquisition (SAMA) Policy" (OCIO 3-110) states that the EDSOC is required to monitor the network for unauthorized software and notify the EARB of any suspected unauthorized software and determine whether the software is/is not approved.[2] It is the responsibility of the IT POC to verify whether there is

[2] Unauthorized software includes pirated software or copyright infringement in the use of software.

a license for the software. If there is no license agreement on record, the IT POC, in conjunction with the ISSO, takes appropriate action to remove any unlicensed software. No employee or contractor can loan, distribute, or transmit Department software to any third party, unless the employee or contractor is expressly authorized to do so by OCIO and the applicable license.

OCIO 3-110 explicitly states that no employee or contractor can install, reproduce, distribute, transmit, download, or otherwise use software for which the Department lacks the appropriate license, unless such software is properly licensed to the employee or contractor, and is approved and used in accordance with Departmental policy and the applicable license. It further states that no employee or contractor can download from the internet or obtain from other sources and install any software that has not been properly tested in accordance with contractor standards on Department computers unless otherwise directed to do so by written authorization from the Chief Information Officer or designated representative.

OCIO 3-110 identifies different levels of responsibilities relating to digital rights management. For instance, it is the employee and contractor's responsibility to ensure that no unlicensed software is installed on the agency computer. EDSOC is responsible for reporting to the PO's ISSO and the employee's supervisor the use of unsolicited software and following up with the EDSOC helpdesk for software blacklisting. Further, EDSOC is responsible for continuously monitoring the Department's network for unlicensed, unapproved, or unauthorized software and providing a weekly report to the EARB on the results. Finally, it is the helpdesk technician's responsibility to ensure that they do not install, or assist in the installation of, unlicensed software on the agency computer.

**(iii)A description of how the covered agency is using the capabilities described in (ii)**

Data Loss Prevention Capabilities

According to the Department, the DLP system deployment was initiated in November 2015, with the actual deployment of data protection software to employee workstations (desktops and laptops) during December 2015 and January 2016. In January 2016, users were notified that they may see different DLP related messages when performing various actions such as transmitting unencrypted SSNs (or numeric strings that appear to be SSNs), as well as transferring large files or content regardless of the existence of SSNs. As the DLP develops, the Department plans on transitioning to proactive blocking of emails containing unencrypted SSNs, preventing the transmission of unencrypted SSNs and protecting users from potential security violations. The sender of the message receives an automated message from the DLP system advising them that their message was blocked and delivery prevented. If the message was an email, the user would receive the automated message in the form of an Automated Notification (in the form of a pop-up notification box) Response Action. If the blocked message was web browser traffic, the user would receive notification directly in their web browser.

According to the Department, during the initial deployment of its DLP tool, if a user sent social security numbers unencrypted, they would be contacted by the EDSOC to validate the data transmission. The EDSOC investigates all events that result in a security alert to determine if what caused the alert was an actual security event. If it is not an actual security event, the

EDSOC has the authority to tune the DLP solution to recognize the event. Otherwise, it initiates security incident handling procedures.

Forensic and Visibility Capabilities

OCIO-14 identifies specific activities that are required of system users and system support personnel regarding forensic and visibility capabilities relating to security incidents. These capabilities are outlined below.

**System User Response Activities**

OCIO-14 explains that users participate in incident containment efforts because they have immediate local access to the workstation or other devices that may have been attacked, allowing them to help limit the damage caused by the attack and preserving valuable evidence. Actions taken by the user may significantly impact the state of the evidence and therefore, should be coordinated with TCD and/or the EDCIRC Coordinator. Also, support personnel (i.e., Help Desk, Computer Security Officer, ISSO, etc.) can direct users to take any of the steps to assist in containing and preserving evidence.

If the Incident Handler or Incident Coordinator determines that the incident might result in a future investigation by TCD, the Incident Handler or Incident Coordinator immediately contacts their Information System Security Manager or Computer Security Officer who would then contact the EDCIRC Coordinator (or designated backup), who would then contact TCD. It's imperative that TCD needs to be involved from the beginning of the incident investigation to ensure that all potential evidence is preserved. The TCD Duty Agent is available to the EDCIRC Coordinator 24 hours a day, 7 days a week, for consultation on these matters.

If it is determined the affected system is a laptop, users are required to seek forensic guidance immediately from their ISSO or Computer Security Officer. For instance, improper power disconnection can drain the backup batteries and cause loss of data, which can cause admissibility issues should the laptop be considered evidence in a criminal investigation.

During the eradication phase of the incident, a determination is made as to whether or not evidence needs to be preserved. In the event that evidence needs to be preserved, the EDCIRC Coordinator coordinates with the OIG for next steps.

**System Support Personnel Response Activities**

System support personnel also maintains a chain of custody (that demonstrates who did what when), including clearly demonstrating each transfer of evidence (e.g., date, time, persons involved). This is especially important in preserving any physical evidence that may be analyzed by the TCD or law enforcement. Because preservation of evidence is vital to the incident response process, no changes should be made to any physical evidence. Evidence that is not preserved may cause the Department to lose valuable data that would assist in the full remediation of incidents, as well as support law enforcement prosecution.

In the incident's identification phase, the Incident Coordinator is responsible for communicating incident-related information and escalating the incident, as appropriate, to management and the EDCIRC Coordinator. The EDCIRC Coordinator reports to the appropriate internal and external parties such as TCD.

In the containment phase of the incident, to prevent any damage to evidence, containment activities should be coordinated with the EDCIRC Coordinator who consults with the TCD. System support personnel performs most incident containment activities, such as (1) documenting all actions performed during the response; (2) keeping all Incident Handlers informed and advising the appropriate parties (e.g., system owners) of progress; (3) ensuring that active measures are taken to stop an ongoing incident (e.g., firewall rule set modifications, email filtering, system disconnection); (4) performing two disk images of a system onto unused media, verifying the integrity of the images, and safely storing the second image for future use as evidence; (5) gathering, analysis, and reviewing of network, system, and application logs to ensure containment efforts were successful and that all systems impacted by the incident have been identified; and (6) changing passwords on compromised systems and systems that interact with the compromised systems.

Eradication is the process of identifying the cause of the incident and mitigating that cause, as well as removing components of an incident. It is important to note that eradication may destroy evidence of the incident and TCD must be involved. Any steps taken in the eradication process must be documented. Recovery steps are to be recorded and reported to include the EDCIRC Coordinator and TCD.

Digital Rights Management Capabilities

OCIO 3-110 states that as part of Information Assurance Services' continuous monitoring program, the EDSOC monitors for unapproved/unauthorized software and a weekly report is generated and sent to the EARB for verification and validation. Any software for which OCIO or the IT POC does not have a license or is not approved is enforced through the Continuous Monitoring program and blacklisted by the EDSOC, until approved by the EARB.

According to OCIO 3-110, the Department is required to provide training to both current and new employees in compliance with the Executive Order 13103, Computer Software Piracy, and this SAMA Policy. Specifically, the Department is required to (1) provide training during employee orientation on SAMA Policy regarding the detection and prevention of piracy and the consequences of violating SAMA Policy and applicable copyright laws; (2) circulate reminders of this SAMA Policy on a bi-annual basis and reminders are posted on the Department's intranet on a quarterly basis; and (3) renew this policy annually as part of the required Department's Security Awareness Program.

OCIO 3-110 also requires OCIO ITPS to develop performance measures to monitor the Department's compliance with Executive Order 13103, CIO Council, and this SAMA Policy on a quarterly basis. EDSOC runs a weekly report on blacklisted and whitelisted software and provide a copy to the EARB for verification and validation. OCIO ITPS runs quarterly reports

on software applications and provide a copy to the EDSOC and the EARB to ensure the Department is in compliance with OCIO 3-110.

**(iv) If the covered agency is not utilizing capabilities described in (ii), a description of the reasons for not utilizing such capabilities**

The Department is utilizing these capabilities described above in (ii).

**(E) Description Of The Policies And Procedures Of The Covered Agency With Respect To Ensuring That Entities, Including Contractors, That Provide Services To The Covered Agency Are Implementing The Information Security Management Practices Described In (D)**

OCIO-01 documents and set forth the Department Information Assurance (IA) Cybersecurity Policy regarding IA/cybersecurity for all IT assets and services operated within or on behalf of the Department. This policy is based on statutory and executive directive requirements that include Federal laws and regulations, Presidential Directives and Executive Orders, National Institute of Standards and Technology Special Publications 800 Series, National Institute of Standards and Technology Federal Information Processing Standards, Office of Management and Budget Circulars, and Department of Homeland Security policy. Violation of this Policy may result in the loss of, or limitations on, use of information resources, as well as disciplinary and/or legal action, including termination of employment or referral for criminal prosecution in accordance with Federal law and Departmental policy. OCIO-01 applies to all Departmental personnel and contractor staff. Additionally, it applies to all Department IT resources; hardware; software; media; facilities; and data owned, managed, or operated on behalf of the Department. Compliance with this Policy is mandatory. All personnel and support contractors must be familiar with, and comply with policy contained in OCIO-01. The IA Cybersecurity Policy is supported through standards, guidance, directives, and other Information Assurance Services governance documents and shall be complied in full.

In addition, LACG v6.1 states that as part of Access Enforcement, per Federal Acquisition Regulation Part 39.101(d), in acquiring IT for access enforcement, agencies shall include the appropriate IT security policies and requirements, including use of common security configurations (e.g., U.S. Government Configuration Baseline and beyond) available from the National Institute of Standards and Technology.