U.S. Department of Energy

Office of Inspector General

Office of Audits and Inspections

SUMMARY REPORT

Department of Energy's Implementation of Selected Controls as Defined in the Cybersecurity Act of 2015

DOE-OIG-16-14

August 2016

Department of Energy
Washington, DC 20585

August 4, 2016

MEMORANDUM FOR THE SECRETARY

FROM: Rickey R. Hass
Acting Inspector General

SUBJECT: INFORMATION: Summary Report on the "Department of Energy's Implementation of Selected Controls as Defined in the Cybersecurity Act of 2015"

BACKGROUND

The mission of the Department of Energy is to help ensure the Nation's security and prosperity by addressing energy, environmental, and national security challenges. The Department, including its contractors, relies on a variety of information resources and technology systems. For instance, the Department's national security systems process classified information to support critical activities related to maintaining the Nation's nuclear weapons stockpile. In addition, unclassified systems that contain sensitive information, such as personally identifiable information (PII), are used to support activities related to financial management, human resources, and health and safety.

The *Cybersecurity Act of 2015* (Act) required the Office of Inspector General (OIG) to report on various aspects of the Department's national security systems and information systems containing PII. This report summarizes the results of our review. To develop the report, we reviewed information related to management of the Department's Federal and contractor-managed systems. We utilized information provided by a sample of Department programs and sites and held discussions with representatives from these locations. Where possible, we leveraged ongoing and prior audit work that was conducted in areas covered by the Act.

RESULTS OF REVIEW

We found that the Department had generally developed and implemented controls related to a number of the areas covered by the Act. However, based on the information reported by the Department, we also noted areas highlighted by the Act where the Department had not fully implemented certain types of controls. In particular:

- We determined that the Department had generally developed policies and procedures related to logical access controls over its national security systems and systems that contain PII. These policies and procedures addressed areas such as account management, separation of duties, unsuccessful login attempts, remote access, and identification and authentication.

- Although we noted an overall lack of policies and procedures related to software license inventories, the Department's programs and sites utilized a range of independent capabilities related to software inventory management.

- We identified mixed capabilities related to the Department's ability to conduct forensic activities and monitor and detect data exfiltration. However, we noted limited to no capabilities related to digital rights management.

Logical Access Policies, Procedures, and Controls

The Act[1] required the OIG to provide a description of the logical access control policies and practices used by the Department over national security systems and systems containing PII, including whether appropriate standards were followed. As a result of our testwork, we determined that the Department had established policies and procedures related to logical access controls over its national security systems and systems containing PII. In particular, programs and sites reviewed had documented logical access procedures and practices that were generally consistent with security requirements defined by applicable Federal laws and regulations such as the *Federal Information Security Modernization Act of 2014*, Office of Management and Budget (OMB) Memoranda, and National Institute of Standards and Technology (NIST) Special Publications (SP). For instance, programs and sites developed policies and procedures in accordance with the Committee on National Security Systems Instruction 1253, *Security Categorization and Control Selection for National Security Systems*, for national security systems and NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. The logical access policies and procedures developed by programs and sites governed areas such as account management, separation of duties, least privilege, unsuccessful login attempts, remote access, and identification and authentication. We found that topics covered within policies and practices generally aligned with NIST guidance related to access controls and identification and authentication controls designed to ensure secure access to information systems and resources.

The Act also required the OIG to provide a description and list of the logical access controls and multifactor authentication used by the Department to govern access for privileged users to national security systems and systems containing PII. We found that five of the six locations reviewed reported that strong multifactor authentication was enforced for all privileged access to information systems and resources; however, we did not validate the Department's assertions as part of this review. While the specific multifactor authentication methods varied among locations, authentication for privileged users was predominantly accomplished using one of the following methods:

- Personal Identity Verification (PIV) Credentials: A common identification badge used by Federal employees and contractors to verify identity.

[1] The *Cybersecurity Act of 2015*, Section 406, Federal Computer Security, Public Law 114-113.

- RSA Token: A token used to perform two-factor authentication employing something the user has and something the user knows. Each token generates a unique authentication code at fixed intervals and is assigned to a specific user.

- CRYPTOCard: A credit card–sized mechanism that generates a one-use-only passcode. A user must enter a private personal identification number into the CRYPTOCard to generate the passcode.

OMB directed that agencies implement the use of PIV, or equivalent credentials, for 100 percent of privileged user accounts by the end of fiscal year 2016. Notably, the Department developed a multifactor authentication implementation approach designed to help achieve compliance with OMB requirements by September 30, 2016. The Department reported that, as of June 30, 2016, the majority of privileged user accounts were utilizing PIV credentials for authentication, a significant increase from when the Department began the initiative.

Programs and sites selected for our review also reported the use of several additional security measures that applied to privileged users accessing national security systems and information systems containing PII. Specifically, security measures for privileged accounts, such as account management, separation of duties, and session management, were documented within system security plans, policies, and program cybersecurity plans. For instance, sites utilized a role-based methodology to ensure that privileged access to information systems was strictly controlled. In addition, officials reported that configuration management tools and other automated mechanisms were in place to ensure that privileged accounts were removed or disabled as necessary. One location reviewed reported that it received alerts when privileged accounts were added or when there had been failed login attempts by privileged users on network infrastructure devices.

Software and License Inventories

The Act required the OIG to report on policies and procedures followed to conduct inventories of software present on national security systems and information systems containing PII and the licenses associated with such software. Although programs and sites reported that they had developed policies and procedures for managing software inventories and licenses, our review of the documentation provided found that the information did not always exist. For instance, we determined that Department Order 200.1A, *Information Technology Management*, indicated that it promoted sound resource management practices related to software acquisition. However, we noted that guidance did not exist related to how the Department should conduct software and license inventories. In addition, at one site reviewed, procedures had been documented that contained software acquisition topics related to blanket order agreements, standards, and approvals, but did not address practices associated with conducting an overall inventory of the software present on information systems and the licenses associated with that software. At another site, although an asset management standard operating procedure had been developed to aid in maintaining an accurate inventory of system software, it did not address the inventory procedures followed to track licenses associated with software. These results were consistent with a previous Government Accountability Office report and findings in our prior audit report on the *Follow-up on the Department of Energy's Acquisition and Maintenance of Software*

Licenses (DOE/IG-0920, September 2014), which concluded that Department-wide software inventory management policies were not developed to encompass best practices, including centralized software license management, tracking of and maintaining a comprehensive inventory using automated tools, and use of cost-effective acquisition decisions.

In addition to policy weaknesses, our review determined that the Department had not implemented a centralized process for managing software and related licenses. In particular, we found that the Department's programs and sites maintained independent capabilities related to software inventory management, ranging from the implementation of an automated software management system to manual tracking using spreadsheets. For example, a software management system at one site limited the use of software licenses to a fixed quantity per product and contained technical controls to prevent users from launching specific software when all licenses were in use. In addition, the site reported that the mechanism was utilized in conjunction with configuration management systems to regularly collect an inventory of installed software. Another location indicated that it maintained an inventory of applications that reside in the cloud computing environment, but noted that application licensing was the responsibility of the system owner.

In response to recommendations made in our prior audit report on the acquisition and maintenance of software licenses, we were informed that the Office of the Chief Information Officer's (OCIO) Energy Information Technology Services (EITS) organization utilized commercial-off-the-shelf software to track EITS-administered software licenses for the common operating environment and used spreadsheets to manage the licenses. An official stated that the tracking, management, and reporting of licenses was done annually at "true up" dates or at renewal times, as applicable.

The importance of maintaining an up-to-date inventory of software licenses to monitor and track usage and reduce unnecessary applications was recently highlighted in OMB Memorandum M-16-12 related to *Improving the Acquisition and Management of Common Information Technology: Software Licensing*. The Memorandum tasked agencies with (1) appointing a software manager responsible for managing all agency-wide commercial and commercial-off-the-shelf software agreements and licenses; (2) maintaining a continual agency-wide inventory of software licenses, including all licenses purchased, deployed, and in use; and (3) analyzing inventory data to ensure compliance with software license agreements, consolidating redundant applications, and identifying other cost-saving opportunities.

Capabilities to Monitor and Detect Exfiltration

The Act required the OIG to report on what capabilities the Department had in place to monitor and detect data exfiltration and other threats, including data loss prevention, forensics and visibility, and digital rights management capabilities. During our review, we noted the Department's programs and sites had implemented mixed capabilities to monitor and detect data exfiltration and other threats. Specifically, our review found that, in the cases where implementation had occurred, each capability was operated in a decentralized manner. In particular, we identified that:

- The Department's elements operated various forensic and visibility capabilities at both the Department and site levels. We noted that a robust defense-in-depth approach was used throughout the Department to protect information and systems and to detect, monitor, investigate, and respond to threats. For instance, the Department's Joint Cybersecurity Coordination Center, managed by the OCIO, was responsible for the coordination of enterprise-level cybersecurity and forensics, including analysis of indicators of compromise for distribution to other cybersecurity professionals. In addition, the National Nuclear Security Administration's (NNSA) Information Assurance Response Center provided similar cyberforensic capabilities and monitoring services for both national security and unclassified systems. We also found that several sites maintained their own capabilities to conduct investigations, perform analysis, and store data/evidence in response to cyber incidents.

- Information provided during our review indicated that various data loss prevention capabilities were utilized on sensitive unclassified and classified systems. For instance, in response to our request, an OCIO official reported that data loss prevention capabilities for Department entities were documented as part of the Trusted Internet Connection (TIC) initiative. The OCIO's EITS was the Department's TIC Access Provider and had incorporated firewall solutions to inspect all content traversing the TIC. Officials indicated that, where possible, inspection capabilities were implemented for content transmitted through encrypted tunnels to provide perimeter protections. While TIC controls helped to provide data loss prevention capabilities, most field locations, including national laboratories, did not access the Internet through the TIC. In fact, officials commented that less than 15 percent of the Department's Internet traffic went through the TIC. In addition, limited scanning of data-at-rest residing on network drives and workstations was performed by the OCIO to identify encrypted PII. However, this type of scanning was not prevalent across the Department. One location also reported that data loss prevention capabilities included dedicated devices and infrastructure monitoring for data loss in the network and email communications and monitoring and detection capabilities that are part of the incident response program. Two locations reported that they had not implemented data loss prevention capabilities.

  We also found that the Department had implemented protections to help prevent data loss on national security systems. In particular, national security systems were physically isolated from the Internet and unclassified networks to prevent data loss. Furthermore, the Department had taken actions to help prevent the loss of classified information as a result of a security breach at Los Alamos National Laboratory in 2006, including enhancing the use of thin-client machines and limiting the use of data ports on classified workstations.

- The programs and sites we reviewed did not utilize capabilities related to digital rights management. Officials indicated that digital rights management capabilities were not used for various reasons. For instance, personnel at two sites reviewed stated that no control or requirement existed for the implementation of digital rights management capabilities. Furthermore, it was noted that funding related to implementing digital rights management had not been identified and, given the mission of the site, the effectiveness

of a digital rights solution in the environment was unknown. Officials at another site reported that because software was downloaded from a vendor's Web site, digital rights management capabilities were conducted by the vendor.

Contractor Assurance Processes

The Act required the OIG to provide a description of policies and procedures the Department maintains to ensure that contractors which provide services to the Department are implementing the information security management practices described in the Act. As one of the largest civilian contracting agencies within the Federal Government, the Department relies on an open and transparent relationship between management and operating (M&O) contractors and Federal Site Offices, which provide oversight of the contractors. Department Order 226.1B, *Implementation of Department of Energy Oversight Policy*, required that the Department's M&O contractors establish a comprehensive and integrated contractor assurance system (CAS), which is a contractor-designed system used to manage performance consistent with contract requirements. Once implemented, the CAS should be used as the framework to assess performance and provide data into the contractor's management decision-making process. The system should also be designed to provide transparency between the M&O contractors and Department officials to ensure alignment across the enterprise to accomplish mission needs and aid the Department in determining the necessary level of Federal oversight. Department Order 226.1B described the requirements for an acceptable and effective CAS to manage operational risks. The directive defined the major operational risks to be covered by the CAS, such as meeting applicable requirements for environment, safety, and health, including quality assurance and integrated safety management; safeguards and security; cybersecurity; and emergency management. The CAS should also incorporate contractor management, contractor governance, and Department oversight systems into a single comprehensive site performance management system.

Furthermore, Department Order 205.1B, *Department of Energy Cyber Security Program*, and NNSA's policy on *Baseline Cyber Security Program*, set forth the requirements for a Department cybersecurity program and an organization-wide Risk Management Approach designed to protect information and systems. The policies direct that the Risk Management Approach must include an analysis of threats/risks; risk-based decisions considering security, cost, and mission effectiveness; and implementation of cybersecurity requirements, processes, and protections that are consistent with guidelines from NIST and the Committee on National Security Systems. Department and NNSA contractors are also required to meet the criteria included in the Contractor Requirements Document portion of the Department's directives, which include establishing and maintaining an effective assurance system that provides appropriate transparency for Federal oversight regarding cybersecurity risk management and overall performance.

SUMMARY

As noted in our report, the Department had generally developed policies and procedures related to logical access controls over its national security systems and systems containing PII. In addition, we determined that the Department operated a decentralized program for managing

software licenses and had not established detailed policies and procedures to guide the program. Rather, programs and sites maintained a range of independent capabilities related to software inventory management. Furthermore, although we noted that mixed capabilities existed related to forensic and data exfiltration capabilities, we noted limited to no capabilities within the Department related to digital rights management.

While we are not making recommendations in this report, we have made recommendations in the past addressing several of the areas covered by the Act, such as the development and implementation of policies and procedures, implementation of security controls, and management of software licenses. In these instances, management generally agreed with the recommendations and indicated that corrective actions would be taken. We noted that, since the issuance of the prior reports, actions had been taken to address numerous recommendations. However, absent improvements to its cybersecurity program, the Department's information and systems will be at a higher-than-necessary risk of compromise, loss, and/or modification. In addition, the lack of effective software management practices could result in excessive expenditures by the Department's programs and sites.

Ongoing and future OIG audits will evaluate many of the areas covered by the Act. For instance, the OIG has an ongoing audit to determine whether the Department effectively implemented multifactor authentication when securing its information systems. In addition, the OIG is currently conducting a review of cybersecurity controls, including access controls, at various locations as part of our annual *Federal Information Security Modernization Act of 2014* evaluation to determine whether the Department's unclassified cybersecurity program adequately protected its data and information systems. Furthermore, we are continuing to plan for future audit work as part of our annual risk-based audit planning process.

Attachments

cc: Deputy Secretary
Under Secretary for Science and Energy
Deputy Under Secretary for Management and Performance
Chief of Staff
Chief Information Officer

OBJECTIVE, SCOPE, AND METHODOLOGY

OBJECTIVE

To determine the Department of Energy's status in implementing policies, procedures, practices, and capabilities as defined in the *Cybersecurity Act of 2015* (Act) for national security systems and systems that provide access to personally identifiable information (PII).

SCOPE

The Act required the Office of Inspector General (OIG) to report on (1) the use of logical access controls over national security systems and systems that provide access to PII; (2) policies and procedures used to conduct inventories of the software present on national security systems and systems that provide access to PII and the licenses associated with such software; and (3) capabilities used to monitor and detect data exfiltration and other threats, including forensic and visibility, data loss prevention, and digital rights management capabilities. To fulfill the requirements of the Act, the OIG conducted this review from March to August 2016 at Department Headquarters in Washington, DC, and Germantown, Maryland, as well as selected field sites. Specifically, information used in support of the review was obtained from the Los Alamos National Laboratory, Los Alamos, New Mexico; Sandia National Laboratories, Albuquerque, New Mexico; and the Pacific Northwest National Laboratory and Hanford Site, Richland, Washington. The sites selected for review were judgmentally based on the number and types of systems at each location. The review was conducted under OIG project number A16TG028.

METHODOLOGY

To accomplish the requirements set forth by the Act, we performed the following procedures:

- Reviewed program- and site-level security policies and practices related to management of access control, software inventory management processes, and the capabilities for monitoring data exfiltration from the Department's Federal and contractor-managed systems;

- Reviewed applicable standards and guidance issued by the National Institute of Standards and Technology pertaining to access control to determine whether the Department's policies and procedures were consistent with the standards and guidance;

- Held discussions with officials from the Department and the National Nuclear Security Administration; and

- Evaluated and incorporated the results of prior audit work conducted by the OIG and the Department's Office of Enterprise Assessments, Office of Cyber and Security Assessments.

The Act did not task the OIG with determining the reasons why deficiencies may or may not have existed within the agency. Furthermore, the OIG was not required to substantiate or test assertions made by the Department's programs and/or sites in response to our review of policies, procedures, and practices.

Management waived an exit conference on August 2, 2016.

PRIOR REPORTS

- Evaluation Report on *The Department of Energy's Unclassified Cybersecurity Program – 2015* (DOE-OIG-16-01, November 2015). The Department of Energy had taken positive actions to improve the security and awareness of the unclassified cybersecurity program. However, the evaluation found that the types of deficiencies identified in prior years, such as issues related to security reporting, vulnerability management, system integrity of Web applications, and account management, continued to persist. The weaknesses identified occurred, in part, because the Department had not ensured that policies and procedures were fully developed and/or implemented to meet all necessary cybersecurity requirements.

- Evaluation Report on *The Department of Energy's Unclassified Cybersecurity Program – 2014* (DOE/IG-0925, October 2014). The Department had taken positive actions to improve the security and awareness of the unclassified cybersecurity program. While the Department made strides to correct previously identified deficiencies, additional effort is needed to ensure that the risk of operating systems are identified and that systems and information are adequately secured. In particular, our fiscal year 2014 evaluation identified weaknesses related to performance metric reporting, patch and configuration management processes, access controls, and system integrity of Web applications. The issues occurred, at least in part, because the Department's programs and sites had not ensured that cybersecurity policies and procedures were developed and properly implemented. In addition, the Department's performance monitoring and risk management programs were not completely effective.

- Audit Report on *Follow-up on The Department of Energy's Acquisition and Maintenance of Software Licenses* (DOE/IG-0920, September 2014). Although the Department had made progress in addressing recommendations from a prior audit, it had not adequately managed the acquisition and maintenance of computer software licenses. We determined that programs and sites routinely paid more than necessary when acquiring software licenses and generally had not maintained an inventory of software to assist with management of licenses. In particular, review of software purchase data for a limited number of software products found that programs and sites spent more than necessary during a 3-year period. Additionally, it was determined that prices paid for software by the Department were often greater than established Government-wide acquisition prices. Furthermore, none of the Federal or contractor sites reviewed were able to provide a complete inventory of software licenses. These issues occurred in part because the Department had not developed and implemented a fully effective strategy for acquiring and managing software licenses. Without improvements to the procurement and management of software licenses, the Department will continue to pay more than necessary for its software, be unable to budget for future software costs, and be at risk for overbuying software.

- Evaluation Report on *The Department of Energy's Unclassified Cyber Security Program – 2013* (DOE/IG-0897, October 2013). The Department had taken a number of positive steps over the past year to correct cybersecurity weaknesses related to its unclassified

information systems. In spite of these efforts, we found that significant weaknesses and associated vulnerabilities continued to expose the Department's unclassified information systems to a higher-than-necessary risk of compromise. Our testing revealed various weaknesses related to security reporting, access controls, patch management, system integrity, configuration management, segregation of duties, and security management. In total, we discovered 29 new weaknesses and confirmed that 10 weaknesses from the prior year's review had not been resolved. The weaknesses we identified occurred, in part, because Department elements had not ensured that policies and procedures were fully developed and implemented to meet all necessary cybersecurity requirements. In addition, the Department continued to operate a less than fully effective performance monitoring and risk management program. Absent improvements to its unclassified cybersecurity program, the Department's information and systems will continue to be at a higher-than-necessary risk of compromise.

- Audit Report on *Follow-up Audit of the Department's Cyber Security Incident Management Program* (DOE/IG-0878, December 2012). The Office of Inspector General found that although certain actions had been taken in response to our prior audit report, we identified several issues that limited the efficiency and effectiveness of the Department's cybersecurity incident management program and adversely impacted the ability of law enforcement to investigate incidents. The issues identified were due, in part, to the lack of a unified, Department-wide cybersecurity incident management strategy. In addition, changes to the Department's incident management policy and guidance may have adversely impacted overall incident management and response by law enforcement and counterintelligence officials. We also found that incident reporting to law enforcement was not always timely or complete, which hindered investigations into events. In the absence of an effective enterprise-wide cybersecurity incident management program, a decentralized and fragmented approach has evolved that places the Department's information systems and networks at increased risk.

FEEDBACK

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We aim to make our reports as responsive as possible and ask you to consider sharing your thoughts with us.

Please send your comments, suggestions, and feedback to OIG.Reports@hq.doe.gov and include your name, contact information, and the report number. You may also mail comments to us:

Office of Inspector General (IG-12)
Department of Energy
Washington, DC 20585

If you want to discuss this report or your comments with a member of the Office of Inspector General staff, please contact our office at (202) 253-2162.