Review of the Department of Homeland Security's Implementation of the Cybersecurity Act of 2015

Homeland
Security

DHS OIG HIGHLIGHTS
Review of the Department of Homeland Security's Implementation of the Cybersecurity Act of 2015

Why We Did This Review

Title IV, Section 406 of the *Cybersecurity Act of 2015* requires Inspectors General to assess agency National Security Systems (NSS) and other systems that provide access to personally identifiable information (PII). We reviewed information security policies and practices for logical access and data protection at the Department of Homeland Security in four key areas, as required by the Act.

What We Recommend

We are making no recommendations.

What We Found

The Department has taken a number of steps to implement provisions in Title IV, Section 406 of the *Cybersecurity Act.* As required by the Act, we examined DHS activities in four key cybersecurity areas. We determined the Department has—

- developed enterprise-wide logical access policies and procedures for its NSS and other systems that provide access to PII, in accordance with appropriate Federal standards;
- applied its process for authorizing systems to operate to ensure logical access controls are implemented and assessed, and ensured multi-factor authentication for privileged users of unclassified systems, and some NSS;
- established software inventory policies, although not all DHS components used data exfiltration protection capabilities to support data loss prevention, forensics and visibility, and digital rights management; and
- not developed policies and procedures to ensure that contractors implement data protection solutions.

DHS and its Components can benefit from additional data protection capabilities and policy to help ensure sensitive PII and classified information are secure from unauthorized access, use, and disclosure. We are submitting this report for informational purposes to the appropriate Congressional oversight committees, as required by the Act. Due to a lack of specific criteria, this report contains no recommendations.

Agency Response

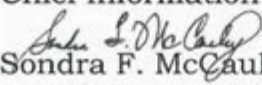We provided a working draft of this report to the Department for review and incorporated DHS' comments as appropriate.

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

September 26, 2016

MEMORANDUM FOR: Jeffrey Eisensmith
                                Chief Information Security Officer

FROM: Sondra F. McCauley
                                Assistant Inspector General
                                Office of Information Technology Audits

SUBJECT: *Review of the Department of Homeland Security's*
                                Implementation of the Cybersecurity Act of 2015

As required by the *Cybersecurity Act of 2015, P. L. No. 114-113, § 406,* dated December 18, 2015, we assessed DHS' information technology security policies, practices, and capabilities for national security systems and systems that provide access to personally identifiable information. We have attached our report, *Review of the Department of Homeland Security's Implementation of the Cybersecurity Act of 2015,* for your information. The report contains no recommendations.

Consistent with our responsibility under the *Inspector General Act,* we will provide copies of our report to congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

Please call me with any questions, or your staff may contact Chiu-Tong Tsang, Director, Cybersecurity and Intelligence Division, at (202) 254-5472.

Attachment

Background

In an effort to improve the security posture of the Federal Government, the President enacted the *Cybersecurity Act of 2015* on December 18, 2015 (*Cybersecurity Act*).[1] The law was designed to establish a mechanism for cybersecurity information sharing among Federal Government and private-sector entities, provide safeguards for private entities that share cybersecurity information, and bolster cybersecurity protections at Federal agencies. The law requires each Inspector General to review and report on four key areas related to agency information technology (IT) security policies and practices for National Security Systems (NSS) and other systems that provide access to personally identifiable information (PII):

1. logical access policies and procedures implemented at the Agency, including whether appropriate standards were followed;[2]
2. logical access controls and multi-factor authentication procedures used to govern access for privileged users;
3. information security management policies for software inventory and data exfiltration protection capabilities;[3] and
4. policies and procedures used to ensure contractors implement data protection services.

As defined in the *Cybersecurity Act*, an NSS is a telecommunications or information system operated by the Federal Government, the function, operation, or use of which involves intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon or weapons system, or is critical to the direct fulfillment of military or intelligence missions. [4]

Within the Department of Homeland Security, the Chief Information Security Officer (CISO) is responsible for managing the enterprise-wide information security program, including establishing IT security policies and procedures for all "Sensitive but Unclassified," "Secret," and "Top Secret" systems. Additionally, the Department's "Top Secret/Sensitive Compartmentalized Information" (e.g., Intelligence systems) fall under the purview of the Office of Intelligence and Analysis (I&A) CISO. Collectively, the DHS CISO and I&A CISO oversee more than 590 information systems, including 56 NSS classified as

---

[1] *Cybersecurity Act of 2015*, Pub. L. No. 114-113, Division N, § 406 (*Cybersecurity Act*).
[2] Logical access involves granting or denying specific requests to obtain and use information and related information processing services.
[3] Data exfiltration protection is a safeguard against unauthorized copying, transfer, or retrieval of data from a computer.
[4] *Cybersecurity Act* § 222, relying on the definition in 40 U.S.C. § 11103, Pub. L. 107–217 (2002).

"Secret," "Top Secret," and "Top Secret/Sensitive Compartmentalized Information," as well as 409 systems that provide access to PII.[5]

While the CISO is responsible for overseeing the enterprise information security program, some of the Department's 22 operational and support Components maintain individual, autonomous IT governance structures. For example, some Component-level CISOs have issued additional, more stringent IT policies and procedures. Consequently, IT practices and implementation of information security capabilities may vary based on a Component's security needs, priorities, and available resources.

Results of Evaluation

The Department has taken a number of steps to implement provisions in Section 406 of the *Cybersecurity Act.* As required, we examined DHS activities in four key cybersecurity areas. We determined the Department has developed enterprise-wide logical access policies and procedures for its NSS and other systems that provide access to PII, in accordance with appropriate Federal standards. DHS has applied its process for authorizing systems to operate to ensure logical access controls are implemented and assessed. It has also ensured multi-factor authentication for privileged users of unclassified systems and most NSS.

Although the Department has established software inventory policies, not all DHS components used data exfiltration protection capabilities to support data loss prevention, forensics and visibility, and digital rights management. Further, the Department had not developed policies and procedures to ensure that contractors implement data protection solutions. DHS components we reviewed generally recognized that additional actions were needed to protect sensitive PII and classified information from unauthorized access, use, and disclosure.

DHS and its Components can benefit from additional data protection capabilities and policy to help ensure sensitive PII and classified information are secure from unauthorized access, use, and disclosure. We are submitting this report for informational purposes to the appropriate Congressional oversight committees, as required by the Act. Due to a lack of specific criteria, this report contains no recommendations.

---

[5] DHS defines NSS as any system that collects, generates, processes, stores, displays, transmits, or receives "Unclassified", "Confidential", "Secret", or "Top Secret" national security information.

Logical Access Policies and Practices

DHS has developed enterprise-wide logical access policies and procedures for its NSS and other systems that provide access to PII, in accordance with appropriate Federal standards. DHS issues IT policies and procedures at the unclassified, classified, and intelligence system levels.[6] Each department-issued policy is used to ensure compliance with the *Federal Information Security Modernization Act*, P. L. No. 113-283 (2014), as well as with guidance from the Office of Management and Budget and the National Institute of Standards and Technology (NIST). DHS' logical access policies include security principles and best practices such as password complexity, least privilege, and segregation of duties to control system access.[7] For unclassified and "Secret" systems, the Department requires two-factor authentication, audit logging capabilities, and encryption for sensitive information throughout its transmission.

DHS' logical access practices are driven by the Homeland Security Presidential Directive 12 (2004). This directive requires multi-factor authentication for logical access through the use of Personal Identity Verification cards issued to its employees and contractors. Personal Identity Verification cards are used for physical access to DHS facilities as well as logical access to its "Sensitive But Unclassified" networks. Moreover, DHS requires the use of security tokens to access the Homeland Secure Data Network (HSDN), which is used to process and store information classified as "Secret".[8]

Logical Access Controls

The Department ensures logical access controls are implemented on its systems through the security authorization process, which entails comprehensive testing and evaluation of the effectiveness of IT security controls. The security authorization process is required for all DHS information systems to obtain authority to operate. The process applies the Risk Management Framework from NIST Special Publication (SP) 800-37 and requires the implementation and assessment of security and privacy controls

---

[6] *DHS Sensitive Systems Policy Directive 4300A,* Version 12.01, dated February 12, 2016; *DHS National Security Systems Policy Directive 4300B,* Version 10.0, dated May 09, 2016; and *DHS Sensitive Compartmented Information Systems Policy Directive 4300C,* Version 1.0, dated September 18, 2013.

[7] The *least privilege* principle requires that users be granted the most restrictive set of privileges needed for performance of authorized tasks, while *separation of duties* ensures the division of roles and responsibilities so that a single individual cannot subvert a critical process.

[8] A security token is a small hardware device that the owner carries to authorize access to a network service. The device may be in the form of a smart card or may be embedded in a commonly used object such as a key fob.

outlined in NIST SP 800-53.[9] Components are required to categorize all of their information systems by potential security impact (low, moderate, high) according to Federal Information Processing Standard 199.[10] Per NIST and DHS guidelines, the potential security impact level determines the security controls and enhancements that must be implemented and documented in the system security plan. Appendix A provides a list of required logical access-related controls.

DHS has accelerated development and implementation of multi-factor authentication policies and practices for privileged users of unclassified systems and some NSS. DHS did so in response to the Office of Management and Budget's June 2015 Cybersecurity Sprint Initiative to combat cyber threats and strengthen the Federal Government's overall cybersecurity infrastructure. As of June 2016, DHS had implemented mandatory Personal Identity Verification use for 99 percent of its privileged accounts and 98 percent of its unprivileged accounts on its Sensitive but Unclassified networks. Additionally, DHS had issued and implemented two-factor authentication tokens to 99 percent of all its required account holders and to 100 percent of its privileged users on HSDN.

While DHS has implemented multi-factor authentication on most of its NSS, some Components continue to operate its NSS with only one authentication factor. A majority of these component systems are stand-alone and unable to implement two-factor authentication. Further, DHS is currently in the process of decommissioning and consolidating some of these NSS for inclusion within the system accreditation boundary of HSDN so they can employ multi-factor authentication. Additionally, the Department has not enabled multi-factor authentication for its intelligence systems. According to I&A CISO officials, the Intelligence Community prohibits the use of multi-factor authentication on Federal intelligence systems.

Information Security Practices and Capabilities

The DHS has established software inventory policies as required. However, due to limited resources, not all DHS components used data exfiltration protection capabilities to support data loss prevention, forensics and visibility, and digital rights management. In addition, we determined that the Department has yet to establish policy requiring Components to implement data loss prevention (DLP) or data rights management (DRM) solutions. However, some components have recognized the need for additional data protection services and plan to either

---

[9] NIST SP 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach*; and NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.
[10] FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems* (2004).

implement or expand DLP and DRM capabilities within the next few years as a means of protecting sensitive PII and classified information from unauthorized access, use, and disclosure.

Software Inventory Policies and Procedures

DHS IT policies and procedures require Components to conduct and maintain software inventories of their information systems as part of the Department's continuous monitoring and security authorization processes. Identification of assets is key to building an accurate and functioning information security continuous monitoring program. As part of continuous monitoring, the CISO collects monthly software asset scanning data from each Component for all unclassified systems and HSDN connected NSS as means of ensuring that all the software being used is authorized. Further, DHS requires that all software installations and updates be preapproved and tracked for configuration management purposes. DHS also requires software licenses to be maintained during the acquisition process and updated or reviewed at least semi-annually.

Data Loss Prevention

DHS has not implemented monitoring and detection exfiltration capabilities department-wide. Only five of nine Components we interviewed operate DLP capabilities on their networks. DLP is defined as the identification and monitoring of sensitive data to ensure that it is only accessed by authorized users and that there are safeguards against data leaks. DLP software provides Components with visibility within their networks, allowing them to identify and flag sensitive information hosted on and outbound from their networks. For example, one Component uses DLP software to identify whether classified data is stored on its unclassified networks. Additionally, one Component uses DLP software to detect PII leaks through emails sent and received.

Forensics and Visibility

Department and Component Security Operations Centers (SOCs) coordinate all incident handling and response. Through the SOCs, DHS has the ability to conduct forensic analysis of all security incidents that occur. For example, the SOCs have end-to-end visibility over the Department's servers, facilitating their ability to investigate incidents to determine scope, evidence of criminal intent, and protective measures needed to minimize future incidents.

Digital Rights Management

DHS has not implemented DRM solutions at all of its Components. DRM refers to the ability to control, manage, and secure information from unauthorized access. DRM can be used to provide additional layers of data protection,

restricting access to authorized users. However, only three of nine Components we reviewed utilized DRM software to protect and restrict sensitive data. Components nonetheless required encryption of sensitive files transmitted externally.

Contractor Data Protection

DHS has not developed policies and procedures to ensure that contractors implement data protection solutions such as DLP or DRM. However, DHS and its Components have established specific IT security guidance for contractors related to safeguarding sensitive information. The Homeland Security Acquisition Regulation and Acquisition Manual serve as the Department's primary sources for contractor guidance.[11] In March 2015, DHS included more stringent security requirements for its contractor information systems that input, store, process, or transmit sensitive information. Since then, contractor information systems must go through the security authorization process and have become subject to independent assessments, reviews, and continuous monitoring.

Conclusion

The Department has taken a number of steps to implement provisions in Section 406 of the *Cybersecurity Act*. For example, the Department has developed enterprise-wide logical access policies and procedures for its NSS and other systems that provide access to PII, according to appropriate Federal standards. DHS ensures logical access controls are implemented and assessed through the security authorization process, and has implemented multi-factor authentication for privileged users of unclassified systems and most NSS. Further, the Department has established software inventory policies. However, not all DHS components utilize or have developed policies to ensure contractors implement data exfiltration protection capabilities.

DHS and its Components can benefit from additional data protection capabilities and policy to help ensure sensitive PII and classified information are secure from unauthorized access, use, and disclosure. We are submitting this report for informational purposes to the appropriate Congressional oversight committees, as required by the Act. Due to a lack of specific criteria, this report contains no recommendations.

---

[11] *Department of Homeland Security Acquisition Regulation,* 48 C.F.R. Chapter 30, dated June 2006; and *Department of Homeland Security Acquisition Manual,* dated October 2009.

Objective, Scope, and Methodology

DHS OIG was established by the *Homeland Security Act of 2002* (P.L.107–296), by amendment to the *Inspector General Act of 1978*. Title IV, Section 406 of the *Cybersecurity Act of 2015* requires the Inspectors General to review NSS and other systems that provide access to PII and submit a report to respective Congressional committees.

We conducted a review to determine whether the DHS and its Components have implemented the logical access policies, controls, and data protection capabilities required by the *Cybersecurity Act*. Our scope included all NSS, as defined by the Act and the Department, and those systems with PII that require a Systems of Records and Notice as determined by the DHS Privacy Office.

To achieve our objective, we interviewed selected officials at the DHS Office of the Chief Information Security Officer and the DHS Privacy Office. We also met with Component IT officials at the Office of Intelligence & Analysis, Customs and Border Protection, U.S. Citizenship Immigration Services, U.S. Immigration and Customs Enforcement, the Federal Emergency Management Agency, the Transportation Security Administration, United States Coast Guard, United States Secret Service, and the Office of Inspector General. Finally, we reviewed policies and procedures, DHS' monthly IT scorecards, security authorization documentation, and system inventories.

We conducted this review between April and August 2016 under the authority of the *Inspector General Act of 1978*, as amended, and according to the Quality Standards for Inspection and Evaluation issued by the Council of the Inspectors General on Integrity and Efficiency. We provided DHS the opportunity to verify the facts of this report and we incorporated their comments as appropriate.

The Office of IT Audits major contributors to this report are Chiu-Tong Tsang, Director; Michael Kim, IT Audit Manager; Amber May, IT Specialist; and Tuyet-Quan Thai, Independent Referencer.

Appendix A
Sample List of Logical Access Controls

Control Number	Control and Enhancement Name
AC-1	Access Control Policy and Procedures
AC-2	Account Management
AC-2(1)	Account Management | Automated System Account Management
AC-2(2)	Account Management | Removal of Temporary / Emergency Accounts
AC-2(3)	Account Management | Disable Inactive Accounts
AC-2(4)	Account Management | Automated Audit Actions
AC-2(7)	Account Management | Role-Based Schemes
AC-2(9)	Account Management | Restrictions on Use of Shared Groups / Accounts
AC-2(12)	Account Management | Account Monitoring / Atypical Usage
AC-2(13)	Account Management | Disable Accounts for High-Risk Individuals
AC-3	Access Enforcement
AC-4	Information Flow Enforcement
AC-5	Separation of Duties
AC-6	Least Privilege
AC-6 (1)	Least Privilege | Authorize Access to Security Functions
AC-6 (2)	Least Privilege | Non-Privileged Access For Nonsecurity Functions
AC-6 (3)	Least Privilege | Network Access to Privileged Commands
AC-6 (5)	Least Privilege | Privileged Accounts
AC-6 (9)	Least Privilege | Auditing Use of Privileged Functions
AC-6 (10)	Least Privilege | Prohibit Nonprivileged Users from Executing Privileged Functions
AC-7	Unsuccessful Logon Attempts
IA-2(1)	Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts
IA-5	Authenticator Management
IA-5(2)	Authenticator Management| PKI-Based Authentication
IA-11	Re-Authentication

Appendix B
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chiefs of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
DHS Chief Information Officer
DHS Chief Information Security Officer
Privacy Office
Component Chief Information Officer
Component Chief Information Security Officer

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees
Senator Orrin G. Hatch

ADDITIONAL INFORMATION AND COPIES

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov. Follow us on Twitter at: @dhsoig.

OIG HOTLINE

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive, SW
Washington, DC 20528-0305