OFFICE OF THE SECRETARY

Review of IT Security Policies, Procedures, Practices, and Capabilities in Accordance with the Cybersecurity Act of 2015

FINAL REPORT NO. OIG-16-040-A

AUGUST 4, 2016

U.S. Department of Commerce
Office of Inspector General
Office of Audit and Evaluation

FOR PUBLIC RELEASE

Contents of APPENDIXES B and C Are Excluded.

UNITED STATES DEPARTMENT OF COMMERCE
Office of Inspector General
Washington, D.C. 20230

August 4, 2016

MEMORANDUM FOR: Steve Cooper
Chief Information Officer

Allen Crawley

FROM: Allen Crawley
Assistant Inspector General for Systems Acquisition
and IT Security

SUBJECT: *Review of IT Security Policies, Procedures, Practices, and Capabilities in Accordance with the Cybersecurity Act of 2015*
Final Report No. OIG-16-040-A

Attached is the final report of our audit of the Department's IT security policies, procedures, practices, and capabilities as defined by the Cybersecurity Act of 2015. This report summarizes our results for logical access controls, multi-factor authentication, software inventory policies and procedures, capabilities to monitor and detect data exfiltration and other threats, and policies and procedures that ensure contractors implement information security management practices for national security systems and systems that provide access to personally identifiable information (PII).

Appendix B of this report, which has been labeled as For Official Use Only, also contains our findings and recommendations related to our work assessing national security systems within the Department.

In response to our draft report, the Department concurred with our recommendations. We have summarized the response and included the entire formal response as appendix C, which has been labeled as For Official Use Only. The final report, with the exception of appendixes B and C, will be posted on OIG's website pursuant to section 8M of the Inspector General Act of 1978 as amended.

In accordance with Department Administrative Order 213-5, please provide us your action plan within 60 days of this memorandum. The plan should outline the actions you propose to take to address each recommendation.

We appreciate the cooperation and courtesies extended to us by your staff during our audit. If you have any questions or concerns about this report, please contact me at (202) 482-1855 or Dr. Ping Sun, Director for IT Security, at (202) 482-6121.

Attachment

cc: Bruce H. Andrews, Deputy Secretary of Commerce
Rod Turk, Director, Office of Cyber Security and Chief Information Security Officer
Catrina Purvis, Chief Privacy Officer
Mike Maraya, Program Manager for Cybersecurity Operations and Analytics; National Security Program Operations; and National and Strategic Cyber Programs
Greg Johnson, National Security Program Operations, Office of the Chief Information Officer
Maria Dumas, Audit Liaison

Report in Brief

AUGUST 4, 2016

OFFICE OF THE SECRETARY

Review of IT Security Policies, Procedures, Practices, and Capabilities in Accordance with the Cybersecurity Act of 2015

OIG-16-040-A

Why We Did This Review

The Cybersecurity Act of 2015 (the Act) requires that each office of inspector general (OIG) submit a report to Congress on the national security systems and systems that provide access to personally identifiable information (PII) operated by or on behalf of its department.

The Act requires the report to include the following areas: logical access policies and practices and logical access controls, multi-factor authentication, software inventory policies and procedures, capabilities to monitor and detect exfiltration and other threats, and policies and procedures that ensure contractors' implementation of information security management practices.

Objective and Scope

The objective of this audit is to examine the IT security policies, procedures, practices, and capabilities—as defined in the Cybersecurity Act of 2015—for national security and PII systems.

While the Secretary of Commerce is ultimately responsible for ensuring the security of the Department's information and information systems, senior officials must manage and supervise the IT security programs in their respective operating units (OUs). For this reason, we examined both the Department and the individual OU IT security policies, procedures, practices, and capabilities.

There are 146 systems that provide access to PII managed by 9 of the 13 OUs within the Department. To conduct our work, we collected and reviewed information on the five areas specified in the Act from each of the 9 OUs: Bureau of Industry and Security (BIS), Census Bureau (Census), International Trade Administration (ITA), National Institute of Standards and Technology (NIST), National Oceanic and Atmospheric Administration (NOAA), National Telecommunications and Information Administration (NTIA), National Technical Information Service (NTIS), Office of the Secretary (OS), and U.S. Patent and Trademark Office (USPTO).

RESULTS ON PII SYSTEMS

We have provided the required descriptions for each of the five areas specified in the Act by identifying common attributes of the IT security policies, procedures, practices, and capabilities across the 9 OUs.

I. *Logical access policies and practices and logical access controls.* In general, logical access policies and practices used by the Department follow appropriate standards, and OUs have asserted logical access controls are in place on most systems. However, we found that NOAA and OS had outdated policies, and Census and USPTO had not fully implemented logical access controls on their systems. More specifically, we found that logical access controls for 10 of the 12 Census systems and 1 of the 4 USPTO systems selected for review were not fully implemented. Census and USPTO developed plans of action and milestones to address the weaknesses identified. As of June 2016, Census has completed the needed corrective actions, and USPTO anticipates completing corrective actions by September 2016.

II. *Multi-factor authentication.* The Act directs OIG to (a) list and describe the multi-factor authentication used by the Department to govern privileged users' access to systems and (b) describe any reasons for not using multi-factor authentication. Our review identified that 5 of the 9 OUs—Census, NIST, NOAA, OS, and USPTO—have not fully implemented multi-factor authentication for privileged users on PII systems.

III. *Software inventory policies and procedures.* The Act directs OIG to describe the policies and procedures followed by the Department to conduct inventories of the software present on the systems. The Department's policy requires that OUs maintain asset inventories for network-connected IT devices, including system software release information. All 9 OUs implement procedures to conduct inventories of the software present on the systems.

IV. *Capabilities to monitor and detect exfiltration and other threats.* The Act directs OIG to describe (a) what capabilities the Department utilizes to monitor and detect exfiltration and other threats, (b) how it is using them, and (c) any reasons for not utilizing such capabilities. We found that all 9 OUs deploy the following capabilities to monitor and detect exfiltration and other threats: external monitoring, security operations centers, intrusion detection systems/intrusion prevention systems, and event correlation tools.

V. *Policies and procedures that ensure contractors' implementation of information security management practices.* The Act directs OIG to describe the policies and procedures of the Department ensuring that contractors are implementing the information security management practices. Contractors that provide IT services to the Department are required to follow the Department's IT Security Program Policy, which specifically requires information system monitoring and software management. Further, the Department requires the IT Compliance in Acquisition Checklist be completed for information system acquisitions.

FINDINGS AND RECOMMENDATIONS

Appendix B, "National Security Systems," presents the results of our review of the Department's national security systems in accordance with the Act. The results, findings, and recommendations contained in appendix B are for official use only.

Contents

Introduction

The Cybersecurity Act of 2015[1] (the Act) requires that each office of inspector general (OIG) submit a report to Congress on the national security systems and systems that provide access to personally identifiable information (PII) operated by or on behalf of its department. The Act requires the report to include the following areas:

- logical access policies and practices and logical access controls,
- multi-factor authentication,
- software inventory policies and procedures,
- capabilities to monitor and detect exfiltration and other threats, and
- policies and procedures that ensure contractors' implementation of information security management practices.

Summary of Objectives, Scope, and Methodology

The objective of this audit is to examine the IT security policies, procedures, practices, and capabilities—as defined in the Cybersecurity Act of 2015—for national security and PII systems.

While the Secretary of Commerce is ultimately responsible for ensuring the security of the Department's information and information systems, senior officials must manage and supervise the IT security programs in their respective operating units (OUs). For this reason, we examined both the Department and the individual OU IT security policies, procedures, practices, and capabilities.

There are 146 systems that provide access to PII managed by 9 of the 13 OUs within the Department (see appendix A, table 2). To conduct our work, we collected and reviewed information on the five areas specified in the Act from each of the 9 OUs:

- Bureau of Industry and Security (BIS)
- Census Bureau (Census)
- International Trade Administration (ITA)
- National Institute of Standards and Technology (NIST)
- National Oceanic and Atmospheric Administration (NOAA)
- National Telecommunications and Information Administration (NTIA)
- National Technical Information Service (NTIS)

[1] Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, div. N, 129 Stat. 2242, 2935-2985 (Dec. 18, 2015). The reporting requirement is contained in section 406.

- Office of the Secretary (OS)
- U.S. Patent and Trademark Office (USPTO)

We validated their reporting on logical access controls, multi-factor authentication, and security monitoring capabilities by examining the latest security control assessment results for a representative subset of 23 systems across the Department. See appendix A for further details regarding our objective, scope, and methodology.

There are eight national security systems in the Department: three managed by OS, one managed by NOAA, and four managed by NTIA. See appendix B for the complete report with findings and recommendations for these systems.

Summary Results on PII Systems

Based on the reporting of the 9 OUs with PII systems, our review identified the following:

- **In general, the OUs' logical access policies and practices follow appropriate standards, and logical access controls are in place on the majority of the selected systems.** However, NOAA and OS have outdated policies, and Census and USPTO did not fully implement logical access controls on their PII systems.

- **More than half (5 of the 9 OUs) have not fully implemented multi-factor authentication for privileged users.** Although Census, NIST, NOAA, OS, and USPTO have not fully implemented the required multi-factor authentication, these OUs have submitted to the Department corrective action plans, which identify the constraints for implementing multi-factor authentication and the date by which the requirement is to be met.

- **All 9 OUs have policies and procedures to conduct software inventory.** The Department's policy requires that OUs maintain asset inventories for network-connected IT devices, including system software release information. All of the OUs implement procedures—through either a fully automated procedure or a combination of automated and manual procedures—to conduct inventories of the software present on the systems.

- **All 9 OUs have capabilities to monitor and detect exfiltration and other threats.** Capabilities include one or more of the following: external monitoring, security operations centers, intrusion detection systems (IDS)/intrusion prevention systems (IPS), data loss prevention tools, and event correlation tools. The Department is in the process of establishing connections with all OUs to the Enterprise Security Operations Center (ESOC), in order to provide enterprise-wide visibility of cybersecurity threats and events.

- **All 9 OUs have policies and procedures to ensure that its contractors implement adequate information security management practices.** Department policy requires the use of an acquisition checklist to ensure that contractor systems meet the Department's IT Security Program Policy. This checklist requires that contractor systems (a) implement security controls and (b) undergo security assessments and an authorization process.

Detailed Results on PII Systems

The structure and content of our results are designed to be responsive to the five areas specified in the Act. We have provided the required descriptions for each area by identifying common attributes of the IT security policies, procedures, practices, and capabilities across the 9 OUs.

I. Logical Access Policies and Practices and Logical Access Controls

The Act directs OIG to describe the logical access policies and practices used by the Department, including whether appropriate standards were followed. Further, the Act requires a description and list of the logical access controls used to govern access by privileged users.

In general, logical access policies and practices used by the Department follow appropriate standards, and OUs have asserted logical access controls are in place on most systems. However, we found that NOAA and OS had outdated policies, and Census and USPTO had not fully implemented logical access controls on their systems.

The Department's IT Security Program Policy contains the logical access control implementation requirements of the Department. This policy is based on the appropriate standard—NIST SP 800-53, revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*—and 7 of 9 OUs have additional logical access policies that follow this standard. Although this standard was published in April 2013, and compliance was expected within 1 year of the publication date, NOAA and OS still have policies and procedures for logical access in place that have not been updated to adhere with this standard. However, NOAA has developed a compliant policy that is in the process of being approved, and OS has a corrective action plan to update its policies by December 2017. Despite these policies being outdated, all 9 OUs have logical access practices that require managers to (a) approve the level of access for new employees and (b) conduct periodic reviews of user access, to determine whether access is still required and in accordance with approved user access documentation.

The technical controls that the OUs use to enforce logical access policies apply to both unprivileged and privileged users of the systems. These controls were determined to be implemented by the latest independent assessment for the selected set of systems reviewed, with the exception of systems at Census and USPTO. We found that logical access controls for 10 of the 12 Census systems and 1 of the 4 USPTO systems selected for review were not fully implemented. Census and USPTO developed plans of action and milestones (POA&Ms) to address the weaknesses identified. As of June 2016, Census has completed the needed corrective actions, and USPTO anticipates completing corrective actions by September 2016.

II. Multi-factor Authentication

The Act directs OIG to (a) list and describe the multi-factor authentication used by the Department to govern privileged users' access to systems and (b) describe any reasons for not using multi-factor authentication. Our review identified that 5 of the 9 OUs have not fully implemented multi-factor authentication for privileged users.

Four OUs—BIS, ITA, NTIA, and NTIS—implement multi-factor authentication for privileged users through the use of a smart card or another software or hardware token. A smart card, such as the HSPD-12 (Homeland Security Presidential Directive-12)–compliant Personal Identity Verification card or Common Access Card, holds the credentials to identify an individual user. A token, be it software or hardware, requires the user to perform an extra step during authentication that demonstrates possession of the token. When accessing a system, the user must physically present a smart card or token (i.e., something the user has) along with a personal identification number (PIN) or password (i.e., something the user knows) to complete authentication. ITA and NTIS require the use of an HSPD-12 compliant smart card, while BIS and NTIA require the use of a software or hardware token.

Although it has been required since 2010,[2] 5 of 9 OUs—Census, NIST, NOAA, OS, and USPTO—still have not fully implemented multi-factor authentication for privileged users on PII systems. In February 2016, the OUs were required to submit corrective action plans to the Department for fully implementing multi-factor authentication through HSPD-12 compliant smart cards. The following have been identified by these OUs as reasons why multi-factor authentication has not been fully implemented:

- **Resource constraints.** These include lacking one or more of the following:
    - funding to purchase and issue a smart card or to implement other multi-factor authentication solution,
    - funding to hire or contract for additional staff needed to implement multi-factor authentication,
    - dedicated staff to implement multi-factor authentication solution, and
    - staff with the technical skills to implement multi-factor authentication.
- **Technical limitations.** These include legacy systems, or system or software incompatibility, that would preclude them from implementing multi-factor authentication.

[2] Multi-factor authentication for privileged users has been a requirement for high impact systems since 2006 and 2010 for moderate and low impact systems. There are nine high impact systems within the Department that provide access to PII, one BIS and eight NOAA systems. With the exception of two low impact systems, the remaining Department systems that provide access to PII are moderate impact.

Table 1. OU Assertions as to Why Multi-factor Authentication Is Not in Place for Privileged Users

Operating Unit	Resource Constraints	Technical Limitations	Date Expected to Fully Implement Multi-Factor Authentication
Census	X		September 2017
NIST		X	September 2017
NOAA[a]		X	September 2016[b]
OS	X		September 2016
USPTO	X	X	October 2016

Source: OIG analysis of Departmental responses

[a] An additional constraint unique to NOAA is that it asserted several systems have not fully implemented multi-factor authentication for privileged users because of the period of time (as long as 6 months) it takes to provision a smart card.

[b] NOAA noted that one of its systems providing access to PII will not meet the requirement by the end of fiscal year 2016, as the system's technology is incompatible with smart card authentication. The agency has not established a corrective action date.

III. Software Inventory Policies and Procedures

The Act directs OIG to describe the policies and procedures followed by the Department to conduct inventories of the software present on the systems.

The Department's policy requires that OUs maintain asset inventories for network-connected IT devices, including system software release information. All 9 OUs implement procedures to conduct inventories of the software present on the systems. We found that the security management practices related to software inventory have been established as either a fully automated procedure or a combination of automated and manual procedures.

Seven OUs—BIS, Census, NIST, NOAA, NTIS, OS, and USPTO—have adopted a combination of technical solutions and manual reviews to identify unauthorized software within the system. These OUs first use tools to identify the software installed on the systems; then security personnel check reports generated by these tools on a periodic basis (e.g., monthly or quarterly) to validate that unauthorized software has not been introduced onto the systems.

Alternatively, ITA and NTIA report that they have adopted a fully automated procedure to conduct software inventory. These two OUs use tools that enforce software baselines by preventing any unauthorized software from running within the system.

IV. Capabilities to Monitor and Detect Exfiltration and Other Threats

The Act directs OIG to describe (a) what capabilities the Department utilizes to monitor and detect exfiltration and other threats, (b) how it is using them, and (c) any reasons for not utilizing such capabilities.

We found that all 9 OUs deploy the following capabilities to monitor and detect exfiltration and other threats: external monitoring, security operations centers, intrusion detection systems (IDS)/intrusion prevention systems (IPS), and event correlation tools. In addition, more than half of the OUs (i.e., BIS, Census, ITA, NTIA, and OS) implement data loss prevention capabilities. Currently, the Department is in the process of establishing connections between all OUs and the ESOC in order to provide enterprise-wide visibility of cybersecurity threats and events. The capabilities deployed by the OUs and how they are used are described below:

- **External monitoring capability.** All OUs have an established agreement with the Department of Homeland Security (DHS) to receive network monitoring through the Einstein program, which provides real-time monitoring and analysis of Internet traffic flowing in and out of federal agencies' networks. Although BIS internet traffic is monitored by Einstein sensors, the system that provides access to PII is not connected to the Internet and therefore does not require this capability.
- **Security Operations Centers (SOCs).** All OUs have established individual SOCs or leverage the security operations center located within the Herbert C. Hoover Building campus. SOC staff review system alerts, logs, and security tools that provide visibility of malicious network activity. SOCs monitoring BIS, NIST, NOAA, and USPTO are staffed around the clock—and SOCs monitoring Census, ITA, NTIA, NTIS, and OS are staffed during business hours 5 days a week.
- **IDS/IPS.** All OUs have IDS/IPS tools to monitor networks or systems for malicious activities or policy violations. They create an alert and may, depending on the tool configuration, stop predefined malicious activity.
- **Event correlation.** All OUs employ event correlation tools or security information and event management (SIEM) tools that allow for the collection and aggregation of information produced by security logs generated throughout the organization. These tools collect security log information from network devices (e.g., routers, switches, firewalls)—as well as servers, applications, and endpoints—and allow for greater analysis of the events and quicker identification of security incidents.
- **Data loss prevention (DLP).** BIS, Census, ITA, NTIA, and OS employ DLP tools that are designed to detect potential data breaches or data exfiltration transmissions and prevent them by monitoring for data signatures that match the type of information. In order to classify certain information as sensitive, these solutions can use mechanisms, such as exact data matching, structured data fingerprinting, rule and regular expression matching, or predefined keywords. NIST, NTIS, and USPTO have plans in place to implement DLP capabilities; NOAA does not implement DLP.
- **ESOC:** This initiative is expected to provide Department-wide, around-the-clock, near real-time cybersecurity status information. The correlation and analysis of cybersecurity threats and events will improve the overall cybersecurity situational awareness for the entire Department. All OUs are in the process of establishing a connection with the ESOC.

V. Policies and Procedures That Ensure Contractors' Implementation of Information Security Management Practices

The Act directs OIG to describe the policies and procedures of the Department ensuring that contractors are implementing the information security management practices.

Contractors that provide IT services to the Department are required to follow the Department's IT Security Program Policy (DOC ITSPP), which specifically requires information system monitoring and software management. Further, the Department requires the IT Compliance in Acquisition Checklist be completed for information system acquisitions. This checklist includes a set of the steps that must be taken to ensure that security considerations are incorporated when contracting for IT services in compliance with the DOC ITSPP.

Summary of Agency Response and OIG Comments

In response to our draft report, the Department concurred with our findings and recommendations presented in appendix B of this report. In addition, the Department noted that it has already made initial improvements since the completion of our review, and plans to develop and implement corrective actions to improve the security posture of the Department's national security systems.

The Department's response is provided in appendix C.

Appendix A: Objectives, Scope, and Methodology

Our audit objective was to examine the IT security policies, procedures, practices, and capabilities—as defined by the Act—for national security systems and PII systems operated by or on behalf of the Department. To accomplish our objective, we

- identified the PII systems and national security systems in the Department by normalizing the Official Department Inventory, the inventory of the Office of Privacy, and the individual OUs reporting to find there are 146 PII systems[3] and 8 national security systems operated by 9 OUs within the Department;
- selected 23 systems[4] to validate the OUs assertions of the logical access controls and security monitoring capabilities of the PII systems;
- collected information from each OU on the five areas specified in the Act[5] as applied overall to their PII systems and national security systems, including the system security plans and security assessments for the 23 selected PII systems;
- interviewed OU personnel, including system owners, IT security officers, IT administrators, and organizational directors and administrators; and
- reviewed the collected information and interview responses to provide a collective response to the Act.

Table 2 shows the number of PII systems by each OU and the systems we selected for further validation.

[3] OIG operates a system that provides access to PII, but it was not assessed as part of this audit and not included in the count of systems. NOAA identified an additional system that provides access to PII after the start of our audit, and it has not been included in this report or count of systems.

[4] At least one system was selected from each of the 9 OUs that provide access to PII. The systems were primarily selected based on the sensitivity of the PII, the number of individuals' PII records (in most cases, more than 50,000) within the system, and if the information pertained to the general public. Systems that provide access to sensitive PII such as Social Security numbers and credit card numbers were selected before systems that only contain less sensitive PII such as names and mailing addresses.

[5] In the area of information security management, digital rights management capabilities and practices used to conduct inventories of software licenses were not reviewed.

Table 2. Number of Department Systems with PII

Departmental OU	Total Number of Systems with PII	Number of Systems Selected for OIG Review
BIS	1	1
Census	23	12
ITA	5	1
NIST	29	1
NOAA	46	1
NTIA	3	1
NTIS	1	1
OS	7	1
USPTO	31	4
Total	**146**	**23**

Source: OIG analysis of Departmental data

We reviewed each OU's compliance with the following applicable controls, provisions of law, regulation, and mandatory guidance:

- The Federal Information Security Modernization Act of 2014
- IT Security Program Policy, U.S. Department of Commerce, introduced by the Chief Information Officer on September 12, 2014, and applicable Commerce Information Technology Requirements
- Committee on National Security Systems (CNSS) Instruction No. 1253, *Security Categorization and Control Selection for National Security Systems*
- NIST Special Publications:
    - 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
    - 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
    - 800-53A, Rev. 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*
    - 800-59, *Guideline for Identifying an Information System as a National Security System*

We conducted our field work from March 2016 to June 2016. We performed this audit under the authority of the Inspector General Act of 1978, as amended, and Department Organization Order 10-13, dated April 26, 2013, and in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix B: National Security Systems

Contents of this appendix have been removed from the public version of this report, as they have been labeled as For Official Use Only.

Appendix C: Agency Response

Contents of this appendix have been removed from the public version of this report, as they have been labeled as For Official Use Only.

011200000242