The Department Mismanaged, Neglected, and Wasted Money on the Implementation of IT Security Requirements for Its National Security Systems

REDACTED FINAL REPORT NO. OIG-22-023-I

June 15, 2022

~~CONTROLLED UNCLASSIFIED INFORMATION~~

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

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

June 15, 2022

MEMORANDUM FOR: Don Graves
Deputy Secretary of Commerce

FROM: Frederick J. Meny, Jr.
Assistant Inspector General for Audit and Evaluation

SUBJECT: *The Department Mismanaged, Neglected, and Wasted Money on the Implementation of IT Security Requirements for Its National Security Systems*
Redacted Final Report No. OIG-22-023-I

Attached for your review is our final report on the evaluation of the U.S. Department of Commerce's (the Department's) and its bureaus' management of national security systems. Our evaluation objective was to determine whether the Department and its bureaus are managing national security systems in compliance with federal and Departmental information technology security requirements.

We found the following:

I. The Department mismanaged and neglected information technology security requirements for its national security systems.

II. The Department wasted at least $380,000 on a national security system that it did not use.

Please note that appendix B has been labeled as Controlled Unclassified Information (CUI) and should not be publicly distributed. Please note, however, that when the attached CUI is removed, this transmittal memorandum is Uncontrolled Unclassified Information.

On May 26, 2022, we received the Department's response to the draft report's findings and recommendations. In response to our draft report, the Department concurred with all findings and recommendations.

Pursuant to Department Administrative Order 213-5, please submit to us an action plan that addresses the recommendations in this report within 60 calendar days. This final report will be posted on OIG's website pursuant to sections 4 and 8M of the Inspector General Act of 1978, as amended (5 U.S.C. App., §§ 4 & 8M), with redaction of information that is CUI.

We appreciate the cooperation and courtesies extended to us by your staff during our evaluation. If you have any questions or concerns about this report, please contact me at (202) 793-2938 or Dr. Ping Sun, Director for IT Security, at (202) 793-2957.

Attachment

cc: André Mendes, Chief Information Officer
Jason Rodriguez, Chief of Staff, Office of the Deputy Secretary of Commerce
Ryan Higgins, Chief Information Security Officer, OCIO
Joselyn Bingham, Audit Liaison, OCIO
Maria Hishikawa, IT Audit Liaison, OCIO
MaryAnn Mausser, Audit Liaison, Office of the Secretary
Mark B. Daley, Deputy for Acquisition Program Management, Office of the Secretary
Rehana Mwalimu, Risk Management Officer and Primary Alternate Department GAO/OIG Liaison, Office of the Secretary
Densmore Bartly, Audit Liaison, Office of the Secretary
Chanda Norton, Audit Liaison, Office of the Secretary

Report in Brief

June 15, 2022

Background

The U.S. Department of Commerce (the Department) operates national security systems (NSS) within several of its offices and bureaus. NSS are information technology (IT) systems that store, process, or communicate classified information and, by their very nature, represent some of the greatest IT security risks within the Department. Prior to a reorganization in December 2016, the National Security Programs and Operations office within the Department's Office of the Chief Information Officer (OCIO) was responsible for the Department's national security IT program. Following this reorganization, the Department created the National Security Solutions and Services (NS3) team within OCIO, which became responsible for both overseeing the implementation of the Department's national security IT program as well as managing several NSS. In 2019, NS3 underwent a leadership change, and at the end of our fieldwork in January 2022, the NS3 director left his position. In March 2022, the Department Chief Information Officer became the acting NS3 director.

Why We Did This Review

The objective of our evaluation was to determine whether the Department and its bureaus are managing NSS in compliance with federal and Departmental IT security requirements.

OFFICE OF THE SECRETARY

The Department Mismanaged, Neglected, and Wasted Money on the Implementation of IT Security Requirements for Its National Security Systems

OIG-22-023-I

WHAT WE FOUND

We found that the Department mismanaged and neglected IT security requirements for its NSS. We also found that the Department wasted at least $380,000 on an NSS that it did not use. These issues indicate that the Department's national security program has significant deficiencies, which placed these systems at risk and deprived resources from being effectively used. Until the Department takes actions to strengthen efforts to immediately address these deficiencies, longstanding and pervasive issues will likely continue to jeopardize the IT security posture of its NSS.

WHAT WE RECOMMEND

We recommend that the Deputy Secretary of Commerce ensure that the Chief Information Officer does the following:

1. Implement the following Committee on National Security Systems and National Institute of Standards and Technology IT security requirements for System X: (a) fill fundamental security roles (e.g., system owner, information system security officer); (b) complete the risk management framework steps, including authorizing System X to operate; (c) develop a process to regularly install software security updates; and (d) replace end-of-life system components.
2. Implement multi-factor authentication for access to all of the Department's NSS according to Committee on National Security Systems requirements.
3. Define and convey which responsibilities OCIO will provide regarding a multi-factor authentication infrastructure.
4. Perform an organizational review to ensure all of the Department's NSS receive sufficient oversight and resources to conduct required security activities.
5. Immediately develop detailed policies and procedures that will do the following: (a) ensure the authorization process for Departmental NSS is clearly defined and executed according to the risk management framework; (b) require that Department NSS receive regular, independent assessments according to the risk management framework. These policies and procedures must include consideration of security clearance adjudication timeframes for future assessments; and (c) address the creation and maintenance of an NSS inventory. This should include a requirement for all Department bureaus to provide an update when changes occur.

Contents

Cover: Herbert C. Hoover Building main entrance at 14th Street Northwest in Washington, DC. Completed in 1932, the building is named after the former Secretary of Commerce and 31st President of the United States.

Introduction

The U.S. Department of Commerce (the Department) operates national security systems (NSS) within several of its offices and bureaus. NSS are information technology (IT) systems that store, process, or communicate classified information and, by their very nature, represent some of the greatest IT security risks within the Department. Prior to a reorganization in December 2016, the National Security Programs and Operations office within the Department's Office of the Chief Information Officer (OCIO) was responsible for the Department's national security IT program. Following this reorganization, the Department created the National Security Solutions and Services (NS3) team within OCIO, which became responsible for both overseeing the implementation of the Department's national security IT program as well as managing several NSS. In 2019, NS3 underwent a leadership change, and at the end of our fieldwork in January 2022, the NS3 director left his position. In March 2022, the Department Chief Information Officer became the acting NS3 director.

National Security Directive 42 (NSD-42)[1] established a national policy for the security of all federal NSS. In part, NSD-42 created a committee to support the implementation of the national policy. In 2001, under Executive Order 13231,[2] this committee was re-designated as the Committee on National Security Systems (CNSS). The Department is required to follow policies, instructions, and directives issued by the CNSS. Using these CNSS requirements, the Department adopted a baseline set of controls for Department NSS.[3]

Due to the inherently sensitive nature of the programs supported by Department NSS, we have used generalized language within this report to convey our findings. This involved using pseudonyms when discussing specific NSS, as well as not including background information or descriptions of the NSS discussed in this report. Further, we have included a non-public appendix (appendix B) which contains the information necessary for the Department to contextualize the findings and recommendations to improve its NSS programs.

[1] The White House, July 5, 1990. *National Policy for the Security of National Security Telecommunications and Information Systems*, NSD-42. Washington, DC: White House.

[2] The White House, October 16, 2001. *Critical Infrastructure Protection in the Information Age*, E.O. 13231. Washington, DC: White House, sec. 8(c)(iii).

[3] U.S. Department of Commerce, June 2019. *Department of Commerce Information Technology Security Baseline Policy (DOC ITSBP)*, Version 1.0. Washington, DC: DOC, p. 8.

Objective, Findings, and Recommendations

The objective of this evaluation was to determine whether the Department and its bureaus are managing NSS in compliance with federal and Departmental IT security requirements. Our evaluation focused on the management of Department NSS and was limited to an unclassified review of NSS programs. Appendix A provides a more detailed description of our scope and methodology.

We found that the Department mismanaged and neglected IT security requirements for its NSS. We also found that the Department wasted at least $380,000 on an NSS that it did not use. These issues indicate that the Department's national security program has significant deficiencies, which placed these systems at risk and deprived resources from being effectively used. Until the Department takes actions to strengthen efforts to immediately address these deficiencies, longstanding and pervasive issues will likely continue to jeopardize the IT security posture of its NSS.

I. The Department Mismanaged and Neglected IT Security Requirements for Its National Security Systems

CNSS requires the Department to follow a defined process to manage the IT security risks associated with operating NSS. This process—developed by the National Institute of Standards and Technology (NIST) and referred to as the risk management framework[4]—requires the Department to (1) identify the security requirements for the system and then (2) select, implement, and assess the security controls that meet those requirements. Finally, a designated senior official makes a risk-based decision on whether to authorize the system to operate. Each of these steps is fundamental to ensuring the security controls of an IT system are in-place and operating as intended.

A. The implementation of IT security requirements for a Department NSS was neglected for more than 20 years

In 2016, OCIO took responsibility for an NSS (hereafter referred to in this report as "System X") from one of the Department's bureaus. Between 2001 and 2016, System X's IT security posture was unknown to the Department, meaning it had never gone through the risk management process. Since OCIO took ownership of System X in 2016, we found that OCIO had not taken actions to adhere to the risk management framework. This neglect resulted in the IT security of System X being unmanaged for more than 20 years. Specifically—and as required by the risk management framework—System X did not have

- an authorization to operate;

[4] DOC National Institute of Standards and Technology, December 2018. *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, SP 800-37, Rev. 2. Gaithersburg, MD: NIST. Available online at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf (accessed March 3, 2022).

- fundamental security roles filled (e.g., system owner, information system security officer); and
- IT security controls that were selected, implemented, or assessed.

We also found that System X components[5] had not received security updates and were operating with end-of-life software,[6] leaving the system highly vulnerable. Fortunately, System X was stand-alone—i.e., it was not connected to any other computer networks—and resided within a sensitive compartmented information facility (SCIF). However, the SCIF is a shared space that hosts other systems and users who are not authorized to access this particular NSS. While System X was unmanaged and its IT security posture remained unknown, the system could be exploited by an insider threat.[7] Additionally, there was no assurance that controls have been properly implemented to protect the system's classified data and ensure that the system remains stand-alone.

During our fieldwork, we found that the positions of both the NS3 Director and the Office of the Secretary's Chief Information Security Officer were held by the same individual. This individual's dual responsibility contributed to the prolonged neglect of System X by OCIO. According to the NS3 Director, his security staff were spread between the two offices, leaving the staff unavailable to address the security requirements of this system. NS3 officials stated that addressing the issues associated with System X was a low priority considering it was stand-alone. The NS3 Director also stated that he was not aware of this particular NSS until 2021. Even after its Director became aware of this neglected NSS, NS3 did not take fundamental steps to address the IT security of the system, as of our fieldwork in fiscal year (FY) 2022. When combined, these reasons demonstrate that OCIO mismanaged System X since taking responsibility of it in 2016.

B. The Department had not implemented multi-factor authentication to access its NSS

Multi-factor authentication (MFA) is a method of authentication that requires the use of two or more pieces of evidence—i.e., credentials—before a user is allowed access to a system. Credentials fall into any of the following three categories: (1) something a user knows (e.g., a password or a personal identification number), (2) something a user possesses (e.g., a smart card), or (3) something a user is (e.g., a fingerprint). Credentials must come from two different categories to enhance security—thus, entering two

[5] System components include servers and workstation computers.

[6] *End-of-life* signifies that the vendor would no longer provide security patches or maintenance for the product. Under these conditions, the system would be vulnerable to any newly discovered exploits.

[7] An *insider threat* is when a user exceeds their authorized access—wittingly or unwittingly—to do harm to the security of the United States.

different passwords would not be considered multi-factor. The CNSS[8,9] requires all NSS to have MFA implemented for all user access. The Department Information Technology Security Baseline Policy[10] requires the implementation of MFA for its NSS. A recent national security memorandum[11] also requires the implementation of MFA to protect NSS.

We found that MFA has not been implemented for any of the Department's NSS.[12] Although Department NSS were only accessible from within a security facility, access to classified email services was merely protected by a username and password. MFA would reduce the risk of an insider threat stealing another user's credentials to gain unauthorized access to or hide the misuse of classified information. Further, the Department widely implements MFA for access to its unclassified systems. By not implementing MFA, the Department adopted weaker access authentication for its NSS than for its unclassified systems.

In August 2016, OCIO had plans to implement the infrastructure needed to enable MFA on all Department NSS by the end of December 2016. NS3 told us that they performed testing of the MFA infrastructure in 2017, but the project was put on hold and was never resumed. We attempted to understand why this project was put on hold, but NS3 could not explain why and stated that the testing had been performed under prior NS3 leadership. NS3 could also not provide documentation of the 2017 testing. We determined that a change of NS3 leadership in 2019 may have contributed to the MFA infrastructure project not being completed.

MFA was not implemented for any of the Department's NSS because NS3 did not provide the MFA infrastructure and did not communicate the decision to stop the infrastructure project. This infrastructure would have enabled the Department's NSS—including NSS operated by NS3—to meet MFA requirements and ensure adequate protections against insider threats. However, during our fieldwork in FY 2022, NS3 officials stated that NS3 no longer planned to stand up the infrastructure. Nevertheless, we found that Departmental bureaus and offices were still waiting to leverage the MFA infrastructure. For example, one bureau was unaware that NS3 no longer planned to provide the infrastructure. The combination of unimplemented infrastructure and the lack of communication from NS3 have caused MFA to remain unimplemented across the Department's NSS.

[8] Committee on National Security Systems, March 27, 2014. *Security Categorization and Control Selection for National Security Systems*, CNSSI No. 1253. Fort George G. Meade, MD: CNSS, p. D-13. Available online at https://www.cnss.gov/CNSS/issuances/Instructions.cfm (accessed March 3, 2022).

[9] CNSS, September 2021. *Directive On Protecting National Security Systems From Insider Threat*, CNSSD No. 504, Fort George G. Meade, MD: CNSS, Annex A, para. 2.b.i. Available online at https://www.cnss.gov/CNSS/issuances/Directives.cfm (accessed March 4, 2022).

[10] *DOC ITSBP*, B-7-1 and B-7-2.

[11] The White House, January 19, 2022. *Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems*, NSM-8. Washington, DC: White House, sec. 1(b)(iii).

[12] One bureau has implemented controls to compensate for the absence of MFA.

C. *NS3 did not consistently adhere to federal requirements when authorizing its NSS to operate*

NIST's risk management framework requires all federal information systems, including NSS, to be authorized to operate.[13] During our fieldwork in FY 2022, we found that all Department NSS were authorized to operate, except for System X (described in subfinding I.A. of this report). However, we identified significant deficiencies in how NS3 authorized its NSS. A fundamental part of the risk management framework is to have an independent assessor determine if the security and privacy requirements for the system have been implemented. The authorizing official should then make a risk-based decision after being informed by the impartial assessment.

We found that one NSS (hereafter referred to in this report as "System Y"), operated by OCIO since 2012, had never been evaluated by an independent assessor. According to NS3 officials, NS3 lacked the personnel with the required clearance level to perform an assessment because of the lengthy time to complete staff adjudication processes.[14] The Department relied on another federal agency to provide adjudication of security clearances for System Y assessors. NS3 officials stated that this external process contributed to why an independent assessment of System Y had not been completed. Although obtaining security clearances for assessors presented a challenge for NS3, this should not have prevented the security assessment of System Y since 2012. Under these conditions, the authorizing official repeatedly operated System Y with potentially unknown risks. Deficiencies that could have been identified by the independent assessor may have gone unnoticed by OCIO.

We also found that all NSS managed by NS3 had not been consistently authorized to operate for considerable periods of time between 2016 and 2021. This included lapses as long as 11 months, during which systems were not authorized to operate but continued to be used. These lapses occurred because NS3 lacked organizational maturity—as evidenced by a lack of documented processes and procedures—and the inconsistent implementation of its authorization process. By not consistently authorizing these systems to operate, the authorizing official had not verified whether all steps of the risk management framework had been completed, and had not properly reviewed or accepted the risk to the systems. Thus, the Department's most sensitive systems were operated with unknown levels of risk, which could have exceeded the Department's risk tolerance.[15]

[13] The authorize step of the risk management framework includes a decision by the authorizing official based on a review of the security and privacy posture of the system, the risks from the operation or use of the system, and input provided to the authorizing official by organizational officials. An affirmative decision from the authorizing official grants the system an *authorization to operate*.

[14] The *adjudication process* is used by the federal government to determine whether it is in the best interest of national security to grant an individual an eligibility for access to classified information.

[15] *Risk tolerance* is the level of risk or the degree of uncertainty that is acceptable to an organization.

D. The Department's NSS inventory practices were not in accordance with federal law

Since December 2002, federal law has required the Department to maintain an inventory of IT systems, including NSS, and to update it at least annually.[16] Maintaining the contact information for individuals assigned to key security roles for each system is an integral part of this inventory. Between 2017 and 2021, OCIO did not maintain an NSS inventory. In May 2021, NS3 created an inventory of NSS by requesting data, such as the security contacts for each system, from other Department bureaus and offices. However, during our FY 2022 fieldwork, we found that this inventory contained incorrect security contacts for a majority of the Department's NSS.

NS3's inventory contained outdated security contacts because of changes to system personnel. We found that NS3 had no policies for the creation or maintenance of an NSS inventory. This meant that there was no requirement for other Department bureaus and offices to update NS3 when changes occurred to their NSS. Without maintaining an up-to-date inventory containing correct security contacts, OCIO may have difficulty distributing relevant information to the individuals responsible for each of the Department's NSS. For example, the Department's response to security incidents may be delayed because of incorrect contact information.

II. The Department Wasted at Least $380,000 on a National Security System That It Did Not Use

The Federal Information Security Modernization Act of 2014[17] requires the Department to create policies and procedures that ensure NSS comply with federal standards. NS3 was responsible for creating the Departmental policies and procedures that adhere to NSS security requirements. The Investigations and Threat Management Service (ITMS) was a division within the Office of Security responsible for providing investigative capabilities[18] for the Department. ITMS later became an independent office under the Deputy Assistant Secretary for Intelligence and Security in "late 2019 or early 2020".[19] As of September 3, 2021, the Department decided to eliminate ITMS.[20]

In 2017, ITMS procured hardware and software for an NSS. This NSS was intended to be a case management application (CMA) to support ITMS investigations. Between 2018 and

[16] *See* 44 U.S.C. §§ 3505(c) and (c). As noted in 44 U.S.C. § 3505, two subsections for (c) were enacted.

[17] Pub. Law 113-283.

[18] After OIG investigation 19-0714, which included concerns about ITMS authority, the Office of General Counsel concluded on September 3, 2021 that ITMS did not have the full scope of criminal law enforcement and counterintelligence authority that it claimed to exercise.

[19] DOC Office of the General Counsel, September 3, 2021. *Report of the Programmatic Review of the Investigations and Threat Management Service*. Washington, DC: DOC OGC, p. 4. Available online at https://www.commerce.gov/sites/default/files/2021-09/20210903-ITMS-Report.pdf (accessed March 3, 2022).

[20] DOC Office of Public Affairs, September 3, 2021. *U.S. Department of Commerce Accepts Findings and Recommendations from Investigations and Threat Management Service Review* [online]. https://www.commerce.gov/news/press-releases/2021/09/us-department-commerce-accepts-findings-and-recommendations (accessed March 3, 2022).

2021, ITMS spent additional funds on software licensing and product support by exercising extensions to the CMA contract. ITMS also spent money on security testing to authorize the NSS, and ITMS investigators were trained on the use of the CMA software. However, the system was never used by ITMS, nor was any data stored on it. In total, ITMS wasted[21] at least $380,000 during the first 4 years of a 5-year contract. This does not include the time and efforts expended by resource-constrained federal employees while supporting this NSS.

ITMS was previously responsible for implementing a federally required insider threat program for the Department.[22] In FY 2021, prior to its elimination, ITMS exercised the final year of the CMA contract. After deciding to eliminate ITMS, the Office of the Secretary proposed using the CMA in support of a newly formed insider threat program and planned to conduct this program in an unclassified environment.

However, all funds previously wasted cannot be utilized as part of this new insider threat program. According to multiple Office of the Secretary officials, the CMA hardware that was previously part of a classified network cannot be used on an unclassified network. The annual licensing costs during years of non-use cannot be recouped, and the 2018 security assessment can no longer be leveraged because it is no longer current. Additionally, the CMA software training was provided to ITMS—an office that no longer exists.

Mismanagement and dysfunction within ITMS[23] likely contributed to why government funds were wasted, especially during the lead-up to the decision to eliminate ITMS in September 2021. However, NS3 had also not created procedures on how to properly navigate the detailed process of authorizing the NSS, which led to mistakes during the authorization process. For example, ITMS and NS3 realized that the authorization to operate the CMA was granted without completing required privacy steps. Without a documented process, ITMS depended on NS3's knowledge and guidance. Yet, as discussed in subfinding I.C. of this report, NS3 had issues maintaining proper authorizations for its own systems. These circumstances prevented ITMS from using the NSS, and ultimately led to the waste of government funds.

[21] Per *Generally Accepted Government Auditing Standards*, the term "waste" is defined as the act of using or expending resources carelessly or for no purpose and relates primarily to mismanagement, inappropriate actions, and inadequate oversight. *See* U.S. Government Accountability Office, April 2021. *Government Auditing Standards*, GAO-21-368G. Washington, DC: GAO, secs. 6.21, 7.23, and 8.120.

[22] The White House, October, 7, 2011. *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, E.O. 13587. Washington, DC: White House, sec. 2.1(b).

[23] DOC OGC. *Report of the Programmatic Review of the Investigations and Threat Management Service*.

Conclusion

The Department is required to properly implement all CNSS requirements for its NSS, including the risk management framework. Unfortunately, the issues we observed indicate significant IT security deficiencies across multiple aspects of the Department's national security program. These included the disregard of System X for more than 20 years by Department bureaus, the lack of MFA for any of the Department's NSS, the flawed NSS authorization process, and the failure to maintain an NSS inventory. Until the Department takes actions to strengthen efforts to immediately address these deficiencies, longstanding and pervasive issues will likely continue to jeopardize the IT security posture of its NSS.

Recommendations

We recommend that the Deputy Secretary of Commerce ensure that the Chief Information Officer does the following:

1. Implement the following CNSS and NIST IT security requirements for System X:
    a. Fill fundamental security roles (e.g., system owner, information system security officer).
    b. Complete the risk management framework steps, including authorizing System X to operate.
    c. Develop a process to regularly install software security updates.
    d. Replace end-of-life system components.
2. Implement MFA for access to all of the Department's NSS according to CNSS requirements.
3. Define and convey which responsibilities OCIO will provide regarding an MFA infrastructure.
4. Perform an organizational review to ensure all of the Department's NSS receive sufficient oversight and resources to conduct required security activities.
5. Immediately develop detailed policies and procedures that will do the following:
    a. Ensure the authorization process for Departmental NSS is clearly defined and executed according to the risk management framework.
    b. Require that Department NSS receive regular, independent assessments according to the risk management framework. These policies and procedures must include consideration of security clearance adjudication timeframes for future assessments.
    c. Address the creation and maintenance of an NSS inventory. This should include a requirement for all Department bureaus to provide an update when changes occur.

Summary of Agency Response and OIG Comments

On May 26, 2022, we received the Department's response to the draft report's findings and recommendations. In response to our draft report, the Department concurred with all findings and recommendations.

We have included the Department's response as appendix C of this report.

Appendix A: Objective, Scope, and Methodology

The objective of our evaluation was to determine whether the Department and its bureaus are managing NSS in compliance with federal and Departmental IT security requirements.

To do so, we examined systems that have been designated as NSS in accordance with NIST Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*. We interviewed relevant NSS personnel and reviewed documentation from each of the Department's NSS. However, we did not collect or analyze any classified artifacts from these systems. Due to the sensitive nature of NSS, we omitted details that were not essential to our findings, such as system names, locations, missions, and installed software. The details that were not appropriate for public release, but are needed to assist internal stakeholders, are included in appendix B of this report.

Specifically, we worked to determine

1. the security posture and ownership of System X;
2. the authorization to operate status of Departmental NSS;
3. the implementation status of MFA for Departmental NSS;
4. whether the Department is maintaining an accurate inventory of NSS; and
5. applicable laws that govern NSS.

We also reviewed the Department's compliance with the following applicable internal controls, provisions of law, regulation, and mandatory guidance:

- The Federal Information Security Modernization Act of 2014, 44 U.S.C. §§ 3551, et seq.
- U.S. Department of Commerce, *Information Technology Security Baseline Policy*
- NIST Special Publication 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*
- NIST Special Publication 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*
- CNSS policies, directives, and instructions:
    - CNSSD No. 502, *National Directive On Security of National Security Systems*
    - CNSSD No. 504, *Directive on Protection National Security Systems from Insider Threat*
    - CNSSI No. 1253, *Security Categorization and Control Selection for National Security Systems*
    - CNSSI No. 1254, *Risk Management Framework Documentation, Data Element Standards, and Reciprocity Process for National Security Systems*
    - CNSSP No. 25, *National Policy for Public Key Infrastructure in National Security Systems*

We did not solely rely on computer-processed data to perform this evaluation. Although we could not independently verify the reliability of all of the information we collected, we compared the information with other supporting documents to determine consistency and reasonableness. Based on these efforts, we believe the information we obtained is sufficient for the conclusions in this report.

We conducted our evaluation from October 2021 through February 2022 under the authority of the Inspector General Act of 1978, as amended (5 U.S.C. App.), and Department Organization Order 10-13, dated October 21, 2020. We performed our fieldwork remotely or at Departmental locations around the Washington, DC-area.

We conducted this evaluation in accordance with *Quality Standards for Inspection and Evaluation* (December 2020) issued by the Council of the Inspectors General on Integrity and Efficiency. Those standards require that the evidence supporting the evaluation's findings, conclusions, and recommendations should be sufficient, competent, and relevant and should lead a reasonable person to sustain the findings, conclusions, and recommendations. We believe that the evidence obtained provides a reasonable basis for our findings, conclusions, and recommendations based on our evaluation objective.

Appendix B: Expanded Finding Details

The following information provides the Department's OCIO with additional context and details regarding our report findings. These details were not appropriate for public release, but are needed to assist internal stakeholders with implementing our related recommendations.

In 2016, we conducted an audit required by the Cybersecurity Act of 2015,[24] which included a limited review of the Department's NSS.[25] The audit report contained two non-public appendixes. Appendix B included findings and recommendations regarding Department's NSS programs, and appendix C included the Department's response to the report. We encourage OCIO to review these appendices for additional background.

Controlled Unclassified Information (CUI)

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

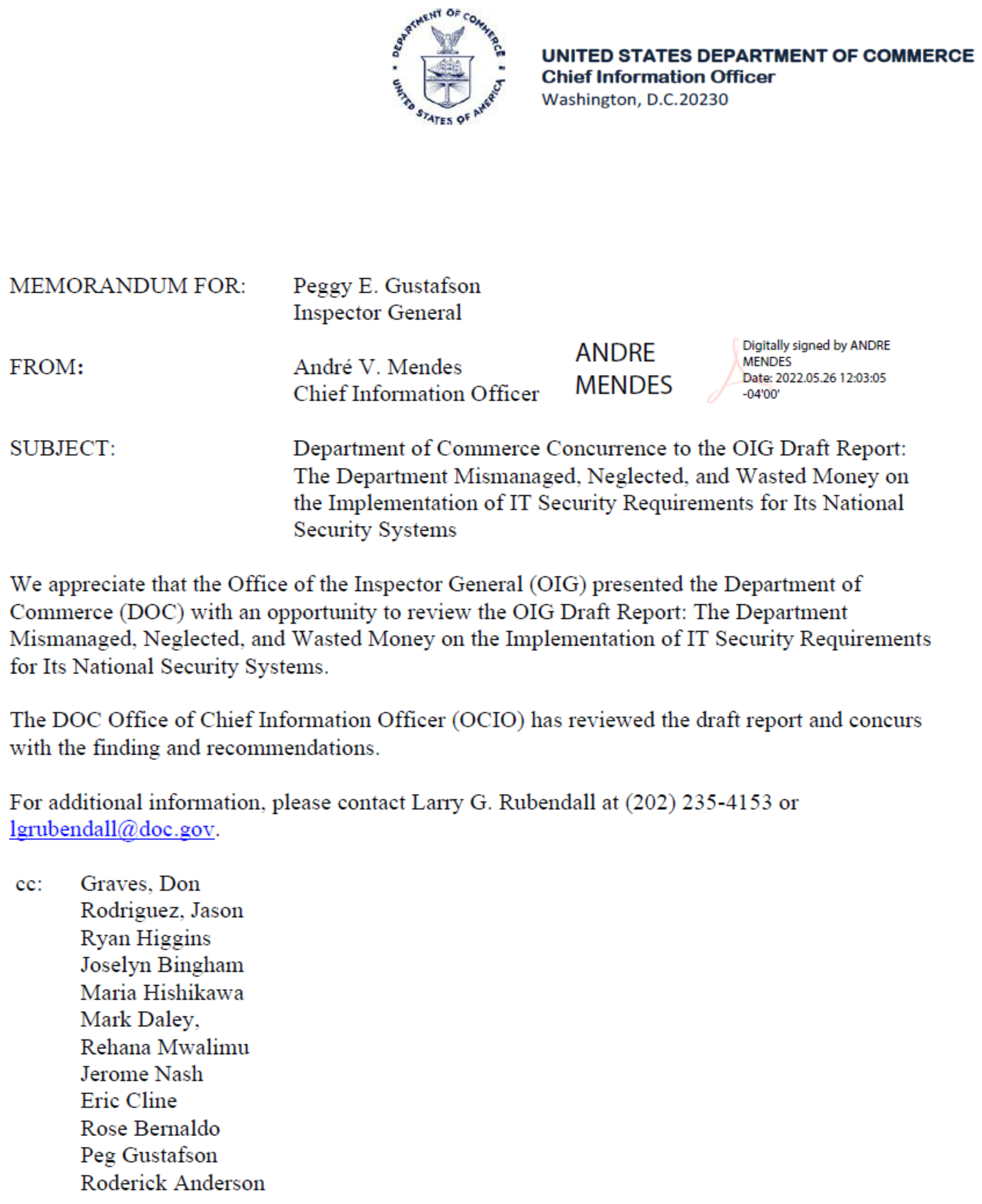
[redacted]

[24] 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.

[25] DOC Office of Inspector General, August 4, 2016. *Review of IT Security Policies, Procedures, Practices, and Capabilities in Accordance with the Cybersecurity Act of 2015*, OIG-16-040-A. Washington, DC: DOC OIG.

Controlled Unclassified Information (CUI)

Appendix C: Agency Response



UNITED STATES DEPARTMENT OF COMMERCE
Chief Information Officer
Washington, D.C.20230

MEMORANDUM FOR: Peggy E. Gustafson
Inspector General

FROM: André V. Mendes
Chief Information Officer

ANDRE MENDES
Digitally signed by ANDRE MENDES
Date: 2022.05.26 12:03:05 -04'00'

SUBJECT: Department of Commerce Concurrence to the OIG Draft Report: The Department Mismanaged, Neglected, and Wasted Money on the Implementation of IT Security Requirements for Its National Security Systems

We appreciate that the Office of the Inspector General (OIG) presented the Department of Commerce (DOC) with an opportunity to review the OIG Draft Report: The Department Mismanaged, Neglected, and Wasted Money on the Implementation of IT Security Requirements for Its National Security Systems.

The DOC Office of Chief Information Officer (OCIO) has reviewed the draft report and concurs with the finding and recommendations.

For additional information, please contact Larry G. Rubendall at (202) 235-4153 or lgrubendall@doc.gov.

cc: Graves, Don
Rodriguez, Jason
Ryan Higgins
Joselyn Bingham
Maria Hishikawa
Mark Daley,
Rehana Mwalimu
Jerome Nash
Eric Cline
Rose Bernaldo
Peg Gustafson
Roderick Anderson

011200000412