# BUREAU OF INDUSTRY AND SECURITY

# Lack of Basic Security Practices Hindered BIS' Continuous Monitoring Program and Placed Critical Systems at Risk

FINAL REPORT NO. OIG-16-003-A

OCTOBER 16, 2015

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

**FOR PUBLIC RELEASE**

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

October 16, 2015

**MEMORANDUM FOR:** Eric L. Hirschhorn
Under Secretary of Commerce for Industry and Security
Bureau of Industry and Security

Allen Crawley

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

**SUBJECT:** *Lack of Basic Security Practices Hindered BIS' Continuous Monitoring Program and Placed Critical Systems at Risk*
Final Report No. OIG-16-003-A

Attached is our final report on the Bureau of Industry and Security's (BIS') continuous monitoring program. Our objective, in accordance with the Federal Information Security Management Act of 2002, was to determine whether BIS' continuous monitoring strategy and practices, including ongoing security control assessments of its critical information systems, provide adequate information for authorizing officials to make proper risk-based decisions.

We found that BIS' documented strategy for continuous monitoring was in compliance with Department policy and NIST guidance. However, BIS did not follow fundamental security practices that are necessary to implement an effective continuous monitoring program for its high-impact systems. Specifically, we found that (1) deficient vulnerability scanning practices increased compromise risk and (2) BIS had no assurance that security weaknesses were remediated.

In response to our draft report, BIS concurred with our five recommendations. We have summarized your agency's response and included its entire formal response as appendix B. The final report 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 with your action plan within 60 days of the date of this memorandum.

We appreciate the assistance and courtesies extended to us by your staff during our audit. If you have any questions about this report, please do not hesitate to contact me at (202) 482-1855 or Dr. Ping Sun, Director for IT Security, at (202) 482-6121.

Attachment

cc: Steve Cooper, Chief Information Officer
Daniel O. Hill, Deputy Under Secretary for Industry and Security
Eddie Donnell, Acting Chief Information Officer, BIS
Rod Turk, Chief Information Security Officer
Ida Mix, Acting Director of Budget, Planning, Assurance and Security, BIS
Mark Crace, Audit Liaison, BIS
Susan Schultz Searcy, Audit Liaison, Office of the Chief Information Officer

# Report In Brief

OCTOBER 16, 2015

## Background

A continuous monitoring program and strategy, required in accordance with Office of Management and Budget (OMB) and Departmental requirements, allows an organization to maintain ongoing awareness of information security vulnerabilities and threats to support organizational risk management decisions. Key components of continuous monitoring are (1) keeping management aware of the current security state of information systems, and (2) supporting the processes of ongoing authorization and near-real-time risk management.

## Why We Did This Review

We conducted this audit to determine whether BIS' continuous monitoring strategy and practices, including ongoing security control assessments of its critical information systems, provide adequate information for authorizing officials to make proper risk-based decisions.

We evaluated BIS' continuous monitoring program, including strategy and implementation. We also performed our own assessments of selected critical security controls in place to protect two of BIS' high-impact systems designed to support its mission to advance U.S. national security, foreign policy, and economic objectives: the BIS Export Control Cyber Infrastructure Version 2 and the Investigative Management System Redesign. We also reviewed BIS' compliance with a number of applicable provisions of law, regulation, and mandatory guidance of, among others, the Federal Information Security Management Act of 2002 (FISMA), IT Security Program Policy, NIST Federal Information Processing Standards, and Special Publications.

## BUREAU OF INDUSTRY AND SECURITY

## Lack of Basic Security Practices Hindered BIS' Continuous Monitoring Program and Placed Critical Systems at Risk

OIG-16-003-A

## WHAT WE FOUND

BIS' documented strategy for continuous monitoring was in compliance with Department policy and NIST guidance. However, we found that

*Deficient vulnerability scanning practices increased compromise risk.* Effective vulnerability scanning supports an organization's continuous monitoring program by allowing the organization to identify vulnerabilities on an ongoing basis. We evaluated BIS' vulnerability scanning practices for its high-impact systems and found significant deficiencies. Specifically, we found that (a) an outdated vulnerability scanning tool was used to identify security weaknesses, (b) required credentialed vulnerability scans were not always performed, (c) vulnerability scanning results were not reviewed to determine remediation actions, and (d) BIS had no assurance that all system components were scanned for vulnerabilities.

*BIS had no assurance that security weaknesses were remediated.* Federal agencies are required to use plans of action and milestones (POA&Ms) to track corrective actions to remediate security weaknesses. In order to create transparency, accountability, and oversight, the Department requires that bureaus use the Department's Cyber Security Assessment and Management (CSAM) tool and follow a standard POA&M process. However, we found that BIS neither consistently followed the required process nor used the required tool to ensure that security weaknesses were remediated. In fact, not only did BIS not take corrective action to address basic IT security weaknesses for over 5 years, it also did not always develop POA&Ms in CSAM to track the known security weaknesses, resulting in avoidance of Department oversight. Furthermore, BIS did not clearly define responsibilities for remediating vulnerabilities.

## WHAT WE RECOMMEND

We recommend that the Under Secretary for Industry and Security direct BIS' acting chief information officer to

1. ensure that an accurate inventory of hardware components and software products that make up its systems is established and maintained.
2. establish an effective vulnerability scanning procedure that requires scanning all components in BIS's inventory, updating the vulnerability scanning tool regularly, using credentials for scanning, and reviewing vulnerability scanning reports in a timely manner.
3. ensure that responsibility for vulnerability remediation, including patching, for BIS system components, is clearly documented.
4. ensure that POA&Ms are created for all un-remediated security weaknesses.
5. implement procedures to provide accountability and greater management oversight of the POA&M process, and ensure supporting artifacts to be included in the POA&Ms.

# Contents

*COVER: Detail of fisheries pediment,*
*U.S. Department of Commerce headquarters,*
*by sculptor James Earle Fraser, 1934*

# Introduction

An information security continuous monitoring program allows an organization to maintain ongoing awareness of vulnerabilities and threats to support organizational risk management decisions. The Department of Commerce's bureaus are required to establish a continuous monitoring strategy and implement a continuous monitoring program in accordance with Office of Management and Budget (OMB) and Departmental requirements. Specifically, bureaus are to manage information security risks on a continuous basis including monitoring the security controls in their information systems, as described in the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) (Special Publication 800-37, Rev. 1). The RMF has sequential steps; continuous monitoring is the final step after the system has been authorized to operate.

Key components of continuous monitoring are (1) keeping management aware of the current security state of information systems and (2) supporting the processes of ongoing authorization and near-real-time risk management. To facilitate the near real-time management of risk associated with information systems, bureaus need to maintain accurate security information about their IT systems. This would include performing security control assessments, remediating identified vulnerabilities, updating the system security plan and security assessment report, and keeping track of security weaknesses and corrective actions on an ongoing basis.

# Objective, Findings, and Recommendations

Our audit objective was to determine whether the Bureau of Industry and Security's (BIS') continuous monitoring strategy and practices, including ongoing security control assessments of its critical information systems, provide adequate information for authorizing officials to make proper risk-based decisions. We evaluated BIS' continuous monitoring program, including strategy and implementation. We also performed our own assessments of selected critical security controls in place to protect two of BIS' high-impact systems, the BIS Export Control Cyber Infrastructure Version 2 (BECCI-2) and the Investigative Management System Redesign.[1] BIS relies on these systems to support its critical mission to advance U.S. national security, foreign policy, and economic objectives by ensuring an effective export control and treaty compliance. See appendix A for further details regarding our objective, scope, and methodology.

BIS' documented strategy for continuous monitoring was in compliance with Department policy and NIST guidance. However, BIS did not follow fundamental security practices that are necessary to implement an effective continuous monitoring program for its high-impact systems. Specifically, we found that (1) deficient vulnerability scanning practices increased compromise risk and (2) BIS had no assurance that security weaknesses were remediated.

[1] For high-impact systems, a security breach could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

# I. Deficient Vulnerability Scanning Practices Increased Compromise Risk

Effective vulnerability scanning supports an organization's continuous monitoring program by allowing the organization to identify vulnerabilities on an ongoing basis. We evaluated BIS' vulnerability scanning practices for its high-impact systems and found significant deficiencies. Specifically, we found that (a) an outdated vulnerability scanning tool was used to identify security weaknesses, (b) required credentialed vulnerability scans were not always performed, (c) vulnerability scanning results were not reviewed to determine remediation actions, and (d) BIS had no assurance that all system components were scanned for vulnerabilities.

## *A. An outdated vulnerability scanning tool was used to identify security weaknesses*

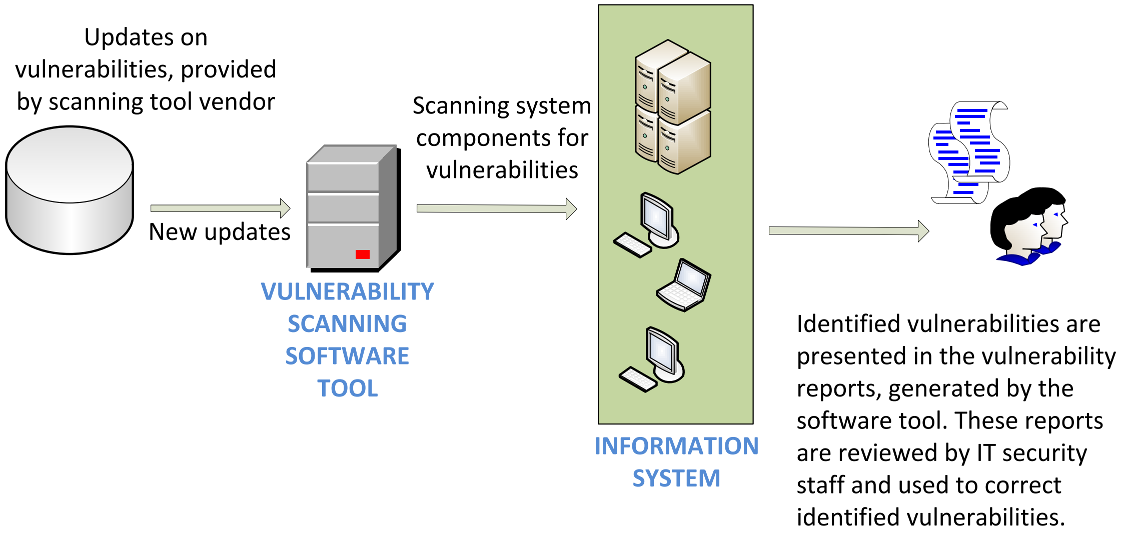
We found that BIS' vulnerability scanning tool had been out of date for 15 months. As a result, the scans performed on the high-impact systems during that time would not have identified any newly discovered vulnerabilities.

A vulnerability scanning tool is essential to help an organization identify vulnerabilities, such as missing software patches, within its systems. In order to work properly, the vulnerability scanning tool must be regularly updated so that it can identify the latest vulnerabilities. According to the tool vendor, in a typical week, the vendor made available dozens of software updates that check for new vulnerabilities (see figure 1, next page). Thus, with the outdated scanning tool, all BIS' vulnerability scans performed on its high-impact systems could not identify new vulnerabilities, increasing the compromise risk for these systems.

Because of the critical risks that emerged in this finding, we quickly issued a memorandum to BIS' Deputy Under Secretary to notify bureau leadership of this problem.[2] In response to our memorandum, BIS updated its vulnerability scanning tool.

[2] U.S. Department of Commerce Office of Inspector General, June 26, 2014. *Use of Outdated Vulnerability Scanning Tool*, memorandum to BIS. Washington, DC: DOC OIG.

**Figure 1. Sample Vulnerability Scanning Process**


Updates on vulnerabilities, provided by scanning tool vendor
New updates
VULNERABILITY SCANNING SOFTWARE TOOL
Scanning system components for vulnerabilities
INFORMATION SYSTEM
Identified vulnerabilities are presented in the vulnerability reports, generated by the software tool. These reports are reviewed by IT security staff and used to correct identified vulnerabilities.

*Source:* OIG

### *B. Required credentialed vulnerability scans were not always performed*

BIS did not properly conduct credentialed vulnerability scans, as required by Departmental policy. Using credentials for vulnerability scanning is essential to effectively identify vulnerabilities on a system. With credentials, which provide administrator-level privileged access to system components, a vulnerability scanning tool can perform an in-depth examination of a system to identify vulnerabilities.

We reviewed reports from the scans BIS conducted on its high-impact systems and found that the credentials were not successfully applied on all components scanned. For example, for the scans conducted in June 2014 and March 2015, only about 50 percent of the system components assessed were appropriately scanned using credentials. Consequently, these scans were not able to thoroughly examine the systems for critical vulnerabilities and therefore did not accurately represent BIS' security posture. According to BIS IT staff, after we briefed them on this issue, the bureau began working to ensure that credentials will be applied on all system components scanned in the future.

### *C. Vulnerability scanning results were not reviewed to determine remediation actions*

Upon completing a scan, the software tool generates reports that provide detailed scanning results, including identified vulnerabilities and their associated security risks. Although BIS scanned its high-impact systems every month, the scanning reports were not reviewed for over a year to validate vulnerabilities identified on the systems and determine remediation actions to fix them. As a result, BIS remained unaware of existing vulnerabilities that made its high-impact systems vulnerable to cyber attacks. Further, regular review of the scanning reports would have made BIS aware of both the issue with the outdated scanning tool and improper credentialed scans, because the related information was also presented in the reports.

When we inquired why these scanning reports were not being reviewed, BIS security staff told us that they were overwhelmed by other priorities, such as correcting security weaknesses identified during assessments to support the last system authorization, and thus did not have time to review them. After we discussed this issue with BIS, its security staff began reviewing vulnerability scanning reports weekly.

### *D. BIS had no assurance that all system components were scanned for vulnerabilities*

BIS could not verify which system components, such as servers and workstations, and software applications are used to support its high-impact systems, because it did not have an inventory of the hardware components and software products that make up its systems. Developing and maintaining an accurate system inventory is a basic, and required, security control. Without a system inventory, BIS had no assurance that all components of its high-impact systems were scanned for vulnerabilities.

When we requested a system inventory for conducting our own vulnerability assessment on BIS' high-impact systems, BIS informed us that the inventory was not available and would be difficult to obtain. In fact, one BIS official told us it would require gathering information from multiple sources, such as network management and vulnerability scanning reports, to compile even an approximate inventory.

Because no system inventory existed, we had to review the system documentation, prior vulnerability scans, and system logging information to identify individual system components. We then selected 28 components for our vulnerability scan at a BIS facility, three of which had not been scanned for more than a year. Our scans found two of these three had critical and high vulnerabilities. We also discovered that no one at the facility knew passwords to log on to a server component that we selected to scan. As a result, we were not able to perform a credentialed scan on it. Apparently, this component had been left running on the system unmanaged for some time.

Not having a system inventory for high-impact systems has been a long-standing issue at BIS. We raised concerns about the same issue on BECCI-2 in 2009.[3] According to BIS, one reason for not having an inventory was that BIS did not have a process in place to coordinate the activities to collect needed information for a system inventory. BIS's IT security staff was responsible for developing and maintaining an inventory; however, developing such an inventory required coordination with other groups, including operations and procurement. Unfortunately, this coordination has not been effective. Currently, BIS is in the initial stage of developing a comprehensive inventory.

[3] DOC OIG, September 30, 2009. *FY 2009 FISMA Assessment of Bureau Export Control Cyber Infrastructure, Version 2*, OSE-19575. Washington, DC: DOC OIG.

## II. BIS Had No Assurance That Security Weaknesses Were Remediated

Federal agencies are required to use plans of action and milestones (POA&Ms) to track corrective actions to remediate security weaknesses. In order to create transparency, accountability, and oversight, the Department requires that bureaus use the Department's Cyber Security Assessment and Management (CSAM) tool and follow a standard POA&M process.[4] However, we found that BIS neither consistently followed the required process nor used the required tool to ensure that security weaknesses were remediated. In fact, not only did BIS not take corrective action to address basic IT security weaknesses for over 5 years, it also did not always develop POA&Ms in CSAM to track the known security weaknesses, resulting in avoidance of Department oversight. Furthermore, BIS did not clearly define responsibilities for remediating vulnerabilities.

### *A. Corrective actions were not taken to remediate security weaknesses*

BIS did not remediate basic IT security weaknesses identified in 2009. In our previous audit we found that BIS Export Control Cyber Infrastructure, Version 2, had significant deficiencies.[5] In response to our recommendations, BIS developed POA&Ms to address these deficiencies. Although BIS asserted that corrective actions were completed and the POA&Ms were marked as closed in 2011, we still found the same types of issues on the same system. Specifically, we found that BIS had not accomplished the following:

- *Take basic steps to establish system inventories*. These inventories would list what hardware components and software products make up its systems (see also finding 1 subfinding D of this report).

- *Adequately define its security requirements*. For example, we found security control implementation descriptions that (1) did not identify the specific details of how to implement the security controls, such as which IT components of the system have logging capabilities and what information would be logged; (2) lacked key security information, such as which network ports, protocols, or services are prohibited on the system; and (3) inaccurately described the security tools used to implement controls when in fact BIS had not used these tools for over a year.

- *Follow the recommendation to obtain the required authorizing officials' approval for system security plans*. The authorizing official's approval of the system security plan represents an important milestone in both the risk management process and the system development life cycle. By approving the plan, the authorizing official agrees to the set of security controls proposed to meet the security requirements for the system.

[4] Commerce Information Technology Requirement CITR-018, POA&M Management, March 5, 2012.

[5] DOC OIG, September 30, 2009. *FY 2009 FISMA Assessment of Bureau Export Control Cyber Infrastructure, Version 2*, OSE-19575. Washington, DC: DOC OIG.

We reviewed the closed POA&Ms that were created to address these weaknesses discussed above and found that (1) the POA&Ms were closed solely based on policy updates, without having remediated the actual security weaknesses; (2) there were no artifacts provided to support the claims that the corrective actions had been taken; and (3) the POA&Ms did not identify who was responsible for implementing the corrective actions nor record who authorized the POA&M closure.

These closed POA&Ms provide no assurance that planned corrective actions were taken to address the identified security weaknesses. In addition, because no record indicated who was responsible for fixing the weaknesses or authorizing closure of the POA&Ms, there was no accountability for correcting known security weaknesses. Lack of accountability in managing POA&Ms is one reason we continue to find the same basic security weaknesses on BIS systems we reported in 2009.

### *B. Corrective actions were not always developed for known security weaknesses*

In September 2013, as part of BIS' process to grant the high-impact systems an authorization to operate (ATO), its independent assessors performed a security control assessment and reported the identified security weaknesses (e.g., system misconfigurations and the use of unnecessary system services) to BIS. However, we found that, after BIS' systems were granted an ATO, BIS did not develop corrective actions for the identified security weaknesses and track them in POA&Ms until after we questioned BIS's POA&M process.

This inaction on the part of BIS had undermined the bureau's security posture. As noted earlier in finding I, we immediately notified BIS when we found that its vulnerability scanning tool was severely out of date. In fact, the same issue was also identified during the 2013 independent security assessments—and explicitly alerted to BIS' IT security staff, acting chief information officer (CIO), and the authorizing official by the independent security control assessors. Nonetheless, no POA&M was created for this security weakness; consequently, it was ignored until we identified the same issue almost a year later.

Proper use of POA&Ms should help BIS keep track of identified security weaknesses and related corrective actions, as well as prioritize resources to fix them in a timely manner. BIS's senior management is responsible for ensuring this process is effectively followed. In addition, tracking POA&Ms in CSAM should allow for management oversight by both BIS and the Department. By not developing and tracking its corrective action plans in CSAM, BIS not only was unaware of the ongoing risks to its IT systems but remained out of the Department's oversight.

### *C. Remediation responsibilities were not defined*

The timely installation of software patches is a critical step toward remediating security vulnerabilities. We found that BIS did not clearly assign responsibilities to do so, resulting in a large number of critical vulnerabilities existing on its high-impact system components. Among the 28 system components we scanned, 23 components are used by the IT operations group to support mission critical infrastructure and applications and 5 by the security staff to support security monitoring and assessment functions. Our vulnerability scans identified more than 400 critical- and high-risk vulnerabilities. More than 70 percent of both critical- and high-risk vulnerabilities were found on the components used by the security staff; many of these vulnerabilities were because of missing patches.

We discussed the results of our scans with both the operations group and the security staff—and learned that each thought that the other group was responsible for patching the components used by the security staff. As a result, the components responsible for providing critical security functions for BIS' high-impact systems were themselves the most vulnerable. We briefed BIS on this issue, and the acting CIO has since clearly established responsibility for securing the system components.

The findings presented in this report raise our concerns about BIS' commitment to follow fundamental security practices required for implementing an effective continuous monitoring program. Until BIS leadership gives serious attention to effectively implementing fundamental security practices, its continuous monitoring program will not provide adequate information for BIS authorizing officials to make risk-based decisions. As a result, BIS systems are more likely to be vulnerable to cyber attack.

## *Recommendations*

We recommend that the Under Secretary for Industry and Security direct BIS' acting chief information officer to

1. ensure that an accurate inventory of hardware components and software products that make up its systems is established and maintained;

2. establish an effective vulnerability scanning procedure that requires scanning all components in BIS's inventory, updating the vulnerability scanning tool regularly, using credentials for scanning, and reviewing vulnerability scanning reports in a timely manner;

3. ensure that responsibility for vulnerability remediation, including patching for BIS system components, is clearly documented;

4. ensure that POA&Ms are created for all un-remediated security weaknesses; and

5. implement procedures to provide accountability and greater management oversight of the POA&M process, and ensure supporting artifacts to be included in POA&Ms.

# Summary of Agency Response and OIG Comments

We reviewed BIS' response, included in appendix B. BIS concurs with the recommendations in the report. Its response notes that it has made progress in the areas we have identified—and initiated collaboration with the Department to enhance BIS' cybersecurity posture. An action plan, with tasks and timelines, will be developed that will address the five recommendations identified in the final report to improve the agency's IT security posture.

# Appendix A: Objective, Scope, and Methodology

Our audit objective was to determine whether BIS' continuous monitoring strategy and practices, including ongoing security control assessments of its critical information systems, provide adequate information for authorizing officials to make proper risk-based decisions.

We reviewed internal controls significant within the context of our audit objective and employed a comprehensive methodology to validate BIS' continuous monitoring strategy and practices. Specifically, we

- Reviewed system-related artifacts, including policy and procedures, planning documents, and other material supporting continuous monitoring.
- Interviewed operating unit personnel, including system owners, the IT security officer, IT staff, and management.
- Performed technical assessments of selected critical security controls in place to protect two of BIS' high-impact systems, the BECCI-2 and the Investigative Management System Redesign.

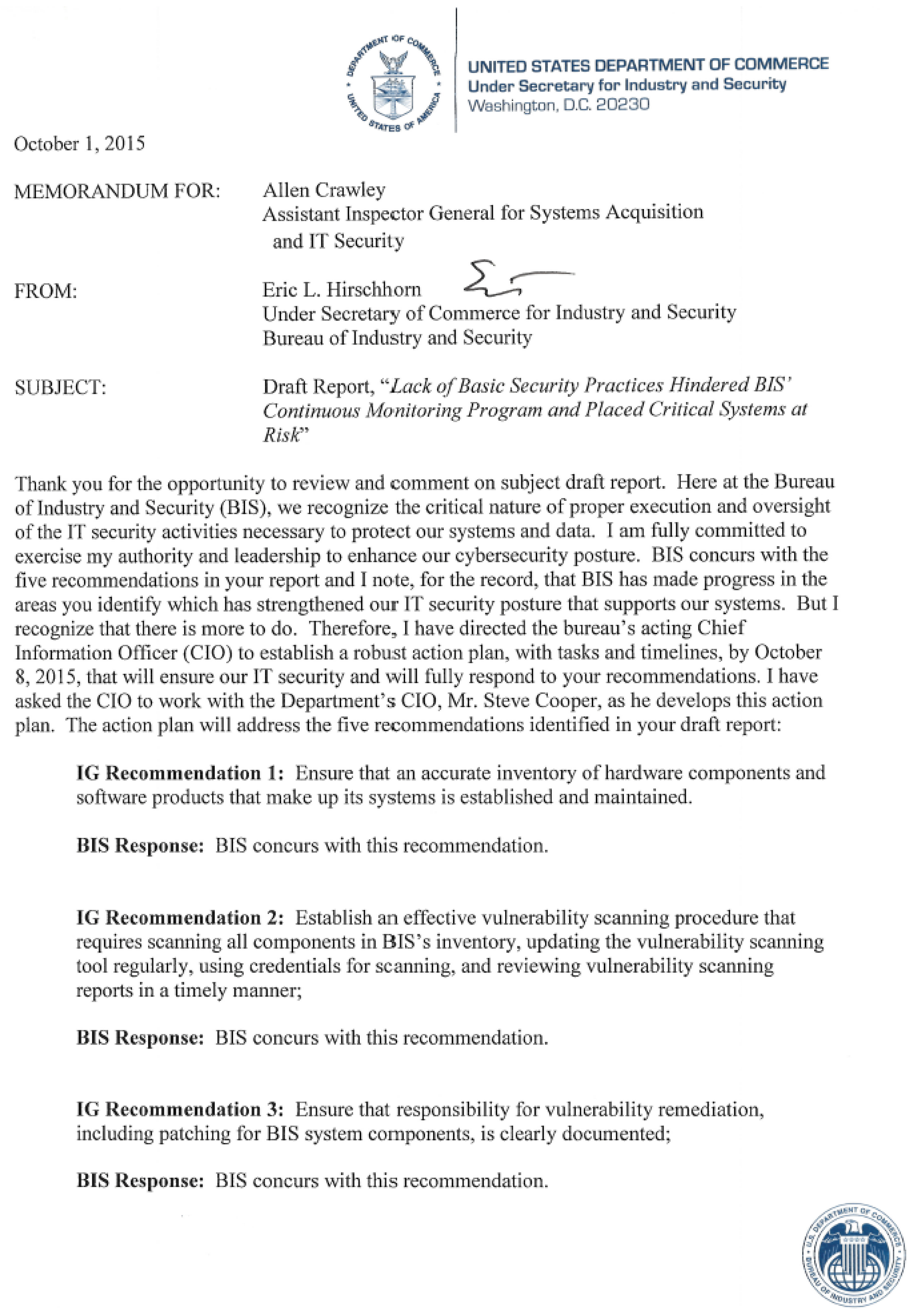
We also reviewed BIS' compliance with the following applicable provisions of law, regulation, and mandatory guidance:

- the Federal Information Security Management Act of 2002
- IT Security Program Policy, U.S. Department of Commerce, introduced by the Chief Information Officer on January 9, 2009, and applicable Commerce Information Technology Requirements
- NIST Federal Information Processing Standards Publications
  - 199, Standards for Security Categorization of Federal Information and Information Systems
  - 200, Minimum Security Requirements for Federal Information and Information 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. 3, Recommended Security Controls for Federal Information Systems and Organizations

- 800-53A Rev. 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans

We conducted our fieldwork from April 8, 2014, to March 9, 2015, at the BIS offices in Washington, DC, and a contractor facility in Manassas, VA. During that time period, sensitive priority assignments necessitated a 6-month suspension of our audit. Fieldwork resumed upon a re-validation of our initial conclusions. 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.

# Appendix B: Agency Response



UNITED STATES DEPARTMENT OF COMMERCE
Under Secretary for Industry and Security
Washington, D.C. 20230

October 1, 2015

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

FROM: Eric L. Hirschhorn
Under Secretary of Commerce for Industry and Security
Bureau of Industry and Security

SUBJECT: Draft Report, "*Lack of Basic Security Practices Hindered BIS' Continuous Monitoring Program and Placed Critical Systems at Risk*"

Thank you for the opportunity to review and comment on subject draft report. Here at the Bureau of Industry and Security (BIS), we recognize the critical nature of proper execution and oversight of the IT security activities necessary to protect our systems and data. I am fully committed to exercise my authority and leadership to enhance our cybersecurity posture. BIS concurs with the five recommendations in your report and I note, for the record, that BIS has made progress in the areas you identify which has strengthened our IT security posture that supports our systems. But I recognize that there is more to do. Therefore, I have directed the bureau's acting Chief Information Officer (CIO) to establish a robust action plan, with tasks and timelines, by October 8, 2015, that will ensure our IT security and will fully respond to your recommendations. I have asked the CIO to work with the Department's CIO, Mr. Steve Cooper, as he develops this action plan. The action plan will address the five recommendations identified in your draft report:

**IG Recommendation 1:** Ensure that an accurate inventory of hardware components and software products that make up its systems is established and maintained.

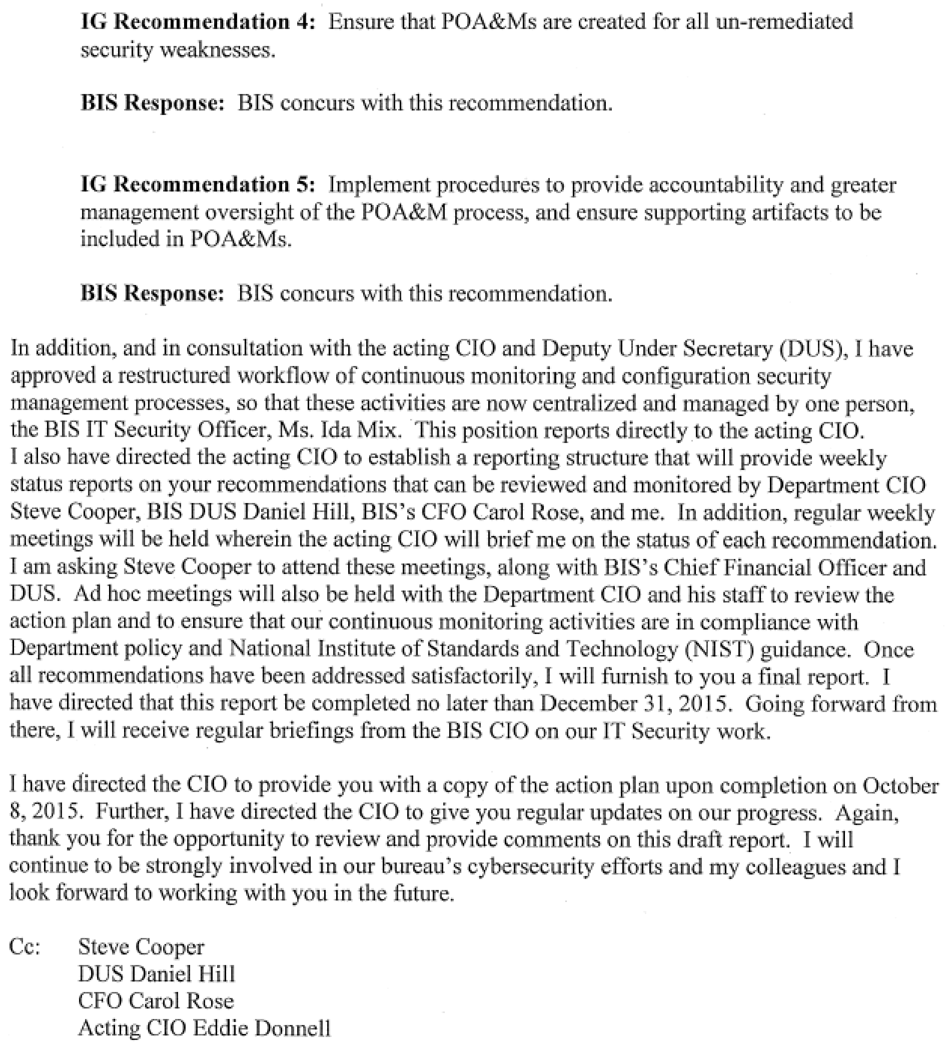
**BIS Response:** BIS concurs with this recommendation.

**IG Recommendation 2:** Establish an effective vulnerability scanning procedure that requires scanning all components in BIS's inventory, updating the vulnerability scanning tool regularly, using credentials for scanning, and reviewing vulnerability scanning reports in a timely manner;

**BIS Response:** BIS concurs with this recommendation.

**IG Recommendation 3:** Ensure that responsibility for vulnerability remediation, including patching for BIS system components, is clearly documented;

**BIS Response:** BIS concurs with this recommendation.



**IG Recommendation 4:** Ensure that POA&Ms are created for all un-remediated security weaknesses.

**BIS Response:** BIS concurs with this recommendation.

**IG Recommendation 5:** Implement procedures to provide accountability and greater management oversight of the POA&M process, and ensure supporting artifacts to be included in POA&Ms.

**BIS Response:** BIS concurs with this recommendation.

In addition, and in consultation with the acting CIO and Deputy Under Secretary (DUS), I have approved a restructured workflow of continuous monitoring and configuration security management processes, so that these activities are now centralized and managed by one person, the BIS IT Security Officer, Ms. Ida Mix. This position reports directly to the acting CIO. I also have directed the acting CIO to establish a reporting structure that will provide weekly status reports on your recommendations that can be reviewed and monitored by Department CIO Steve Cooper, BIS DUS Daniel Hill, BIS's CFO Carol Rose, and me. In addition, regular weekly meetings will be held wherein the acting CIO will brief me on the status of each recommendation. I am asking Steve Cooper to attend these meetings, along with BIS's Chief Financial Officer and DUS. Ad hoc meetings will also be held with the Department CIO and his staff to review the action plan and to ensure that our continuous monitoring activities are in compliance with Department policy and National Institute of Standards and Technology (NIST) guidance. Once all recommendations have been addressed satisfactorily, I will furnish to you a final report. I have directed that this report be completed no later than December 31, 2015. Going forward from there, I will receive regular briefings from the BIS CIO on our IT Security work.

I have directed the CIO to provide you with a copy of the action plan upon completion on October 8, 2015. Further, I have directed the CIO to give you regular updates on our progress. Again, thank you for the opportunity to review and provide comments on this draft report. I will continue to be strongly involved in our bureau's cybersecurity efforts and my colleagues and I look forward to working with you in the future.

Cc: Steve Cooper
DUS Daniel Hill
CFO Carol Rose
Acting CIO Eddie Donnell