OFFICE OF THE SECRETARY

FY 2011 Federal Information Security Management Act Audit: More Work Needed to Strengthen IT Security Department-Wide

FINAL REPORT NO. OIG-12-007-A

NOVEMBER 10, 2011

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

November 10, 2011

MEMORANDUM FOR: Simon Szykman
Chief Information Officer

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

SUBJECT: *FY 2011 Federal Information Security Management Act Audit: More Work Needed to Strengthen IT Security Department-Wide*
Final Report No. OIG-12-007-A

Attached is the final report of our audit of the Department's information security program and practices, which we conducted to meet our obligations under the Federal Information Security Management Act (FISMA). In FY 2011, we assessed the security of 10 systems from three operating units: Census, NOAA, and USPTO.

We found deficiencies in fundamental security planning activities that inhibit the effective implementation of controls. In addition, we identified weaknesses in critical security controls that place the Department's systems at risk. And we found flaws in the Department's Plan of Action and Milestones process that informs risk-based authorization decisions and performance measures for individuals with significant IT security responsibilities.

We are pleased that, in response to our draft report, you concurred with our findings and recommendations. We have summarized your response in the report and included the response as an appendix. We will post this report on the OIG website pursuant to section 8L of the Inspector General Act of 1978, as amended.

Under Department Administrative Order 213-5, you have 60 calendar days from the date of this memorandum to submit an audit action plan to us. The plan should outline actions you propose to take to address each recommendation.

We appreciate the cooperation and courtesies extended to us by your staff as well as operating units' staff during our audit. Please direct any inquiries regarding this report to me at (202) 482-1855, and refer to the report title in all correspondence.

Attachment

cc: Rebecca Blank, Acting Deputy Secretary
Brian McGrath, Chief Information Officer, Census Bureau
Joseph Klimavicz, Chief Information Officer, NOAA
John Owens, Chief Information Officer, USPTO
Catrina Purvis, Chief Information Officer, NESDIS
Larry Tyminski, Chief Information Officer, NMFS
Iftikhar Jamil, Chief Information Officer, NWS
Earl Neal, Director, Office of IT Security, Infrastructure and Technology
Susan Schultz Searcy, Audit Liaison, Office of the Chief Information Officer

Report In Brief

NOVEMBER 10, 2011

Why We Did This Review

Information security program, evaluation, and reporting requirements for federal agencies are established by The Federal Information Security Management Act of 2002 (FISMA). FISMA requires agencies to secure their information systems through the use of cost-effective management, operational, and technical controls. FISMA also requires inspectors general to evaluate agencies' information security programs and practices by assessing a representative subset of agency systems, and to report the results to the Office of Management and Budget (OMB) and Congress annually.

Background

The Department of Commerce's 280 information technology (IT) systems process, store, and transmit census, economic, trade, satellite, and weather data, among others, in support of its varied missions. This year, we assessed the security of 10 information systems selected from three Commerce operating units: five from the National Oceanic and Atmospheric Administration (NOAA), three from the U.S. Patent and Trademark Office (USPTO), and two from the Census Bureau.

In our FY 2010 FISMA audit, we concluded that the Department had not adequately secured its information systems. The Department concurred with our recommendations and developed an action plan to address them—but had not completed the actions by the FY 2011 audit.

OFFICE OF THE SECRETARY

FY 2011 Federal Information Security Management Audit: More Work Needed to Strengthen IT Security Department-Wide

OIG-12-007-A

WHAT WE FOUND

We identified deficiencies in fundamental aspects of security planning and significant security control weaknesses. These include continued failure to implement key controls that govern system access, securely configure components, patch vulnerable software, and audit and monitor system events. Flaws remain in the Department's process for reporting and tracking the remediation of IT security weaknesses. Overall, the entire Department needs to manage information security with greater rigor and consistency.

Specifically, we found deficiencies in:

- security planning that inhibit effective implementation of security controls;
- critical controls thus placing the department's systems at risk; and
- the Department's Plan of Action and Milestones (POA&M) process that undermine effective remediation of security weaknesses.

WHAT WE RECOMMENDED

To make the Department's information security program and practices more effective, the Department should:

- Complete actions planned in response to our FY 2010 FISMA audit, as quickly as possible.
- Develop a security planning checklist, or other planning tool, to help system owners and authorizing officials complete and maintain comprehensive security plans.
- Determine the feasibility of independent reviews at key steps in the risk management framework to ensure greater rigor and consistency in the security authorization process within the Department's various operating units. Consideration should be given to creating independent review teams with representatives from different operating units to share best practices and promote consistent application of Department policy.

Contents

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

Introduction

The Department of Commerce's 280 information technology (IT) systems process, store, and transmit census, economic, trade, satellite, and weather data, among others, in support of its varied missions. Over time, cyber attacks and other information security threats have risen—including those from sophisticated and well-resourced entities using persistent but difficult-to-detect methods—against both government and private industry. Government-wide, federal agencies are struggling to adequately implement their information security programs according to a recent Government Accountability Office report.[1] Strengthening information security Department-wide to protect critical information systems and data is a top management challenge for Department leadership[2] and requires continued commitment of resources and management attention.

Information security program, evaluation, and reporting requirements for federal agencies are established by the Federal Information Security Management Act of 2002 (FISMA). FISMA requires agency heads to secure systems through the use of cost-effective management, operational, and technical controls. FISMA also requires inspectors general to evaluate agencies' information security programs and practices by assessing a representative subset of agency systems, and to report the results to the Office of Management and Budget (OMB) and Congress annually.

We assessed the security of 10 information systems selected from three Commerce operating units: five from the National Oceanic and Atmospheric Administration (NOAA), three from the U.S. Patent and Trademark Office (USPTO), and two from the Census Bureau. The operating units categorized these systems as high- or moderate-impact, based on how severely a security breach would affect organizational operations, assets, or individuals.[3]

Details of our objective, scope, and methodology are described in appendix A.

We identified deficiencies in fundamental aspects of security planning and significant security control weaknesses. These include continued failure to implement key controls that govern system access, securely configure components, patch vulnerable software, and audit and monitor system events. Further, flaws remain in the Department's process for reporting and tracking the remediation of IT security weaknesses. Overall, the entire Department needs to manage information security with greater rigor and consistency.

Our FY 2011 audit of the Department's web applications[4] also identified significant IT security weaknesses that put applications and information at risk of cyber attack. Both audits reaffirm

[1] U.S. Government Accountability Office, October 2011. *Weaknesses Continue Amid New Federal Efforts to Implement Requirements,* GAO-12-137.
[2] Commerce OIG, October 2011. *Top Management Challenges Facing the Department of Commerce,* OIG-12-003.
[3] National Institute of Standards and Technology, February 2004. *Standards for Security Categorization of Federal Information and Information Systems,* Federal Information Processing Standards Publication 199,
[4] Commerce OIG, October 2011. *Improvements Are Needed for Effective Web Security Management,* OIG-12-002-A.

the need to strengthen IT security Department-wide as a top management challenge. Further, we recommend that the Department continue to report IT security as a significant deficiency in its annual Performance and Accountability Report.

Background

In our FY 2010 FISMA audit,[5] we concluded that the Department's information security program and practices had not adequately secured Department systems. We recommended that Commerce revise its IT security policy by providing more specific control implementation requirements; senior managers focus on effectively and consistently implementing key controls; and security weaknesses that we identified be corrected. We also recommended that the Department revise how it records and tracks plans for remediating IT security weaknesses to include integrity controls, evidence requirements, and management oversight. The Department concurred with our recommendations and developed an action plan to address them, but has not completed the actions to date.

The Department is currently revising its IT security policy based on our recommendations. To comply with revised guidelines from the National Institute of Standards and Technology (NIST), the Department also will transition from assessing a system's security controls every 3 years to emphasizing continuous monitoring. The Chief Information Officer also plans to revise the Department policy for recording and tracking how operating units remedy IT security weaknesses, to ensure the integrity of the process and related performance measures.

We believe these efforts should strengthen the Department's information security program and practices. Until the Department successfully implements the items in its FY 2010 audit action plan, however, we will likely continue to find recurring security weaknesses that undermine the Department's ability to defend its systems and information.

[5] Commerce OIG, November 2010. *Federal Information Security Management Act Audit Identified Significant Issues Requiring Management Attention,* OIG-11-012-A.

Findings and Recommendations

I. Deficiencies in Security Planning Inhibit Effective Implementation of Security Controls

Fundamental steps to managing IT security risk include establishing information system boundaries, allocating security controls among interdependent systems, and describing the intended application of controls. Consistent with many of our previous FISMA reviews,[6] 7 of the 10 systems we reviewed in FY 2011 demonstrated shortcomings in one or more of these essential security planning activities. The persistence of these problems is of particular concern because most of the systems had received more than one security authorization,[7] prior to which their security plans should have been updated by system owners and reviewed by senior managers. Officials use security plans, along with security assessments and plans for remediating vulnerabilities, to make risk-based authorization decisions.

A. Hardware and software components need to be accurately identified to ensure system boundaries are well-protected

The boundaries of information systems need to be well-defined in order to be well-protected. Identifying all hardware and software components within a system is critical to managing security; however, we found the identification of hardware and software was deficient in 4 of the 10 systems we reviewed. As a result, such components could present points of entry for attacks on other valuable system resources.

Examples:

- One operating unit's databases, which support critical applications, were not clearly defined as components of either its infrastructure system or its application system, and our scans of the databases revealed they were not securely configured. We first identified this problem in our FY 2009 review and recommended that the operating unit define which system's boundary contained the databases so the appropriate owner could assess and manage their security. In FY 2011, after we again brought this issue to management's attention, the operating unit finally revised its infrastructure system's boundary to include the databases.

- One system lacked an accurate list of hardware and software components, which must be maintained as part of continuous monitoring practices.

[6] We encountered one or more of these three issues in 31 of the 41 (76 percent) systems we reviewed in the previous 4 years' system assessments (FY 2007–FY 2010).

[7] A security authorization is the official management decision of a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the nation based on the implementation of an agreed-upon set of security controls. Reauthorizations can be time-driven (after the authorization period expires, which is typically between 1 and 3 years) or event-driven (when there is a significant change to the information system). See NIST SP 800-37 (cited in appendix A).

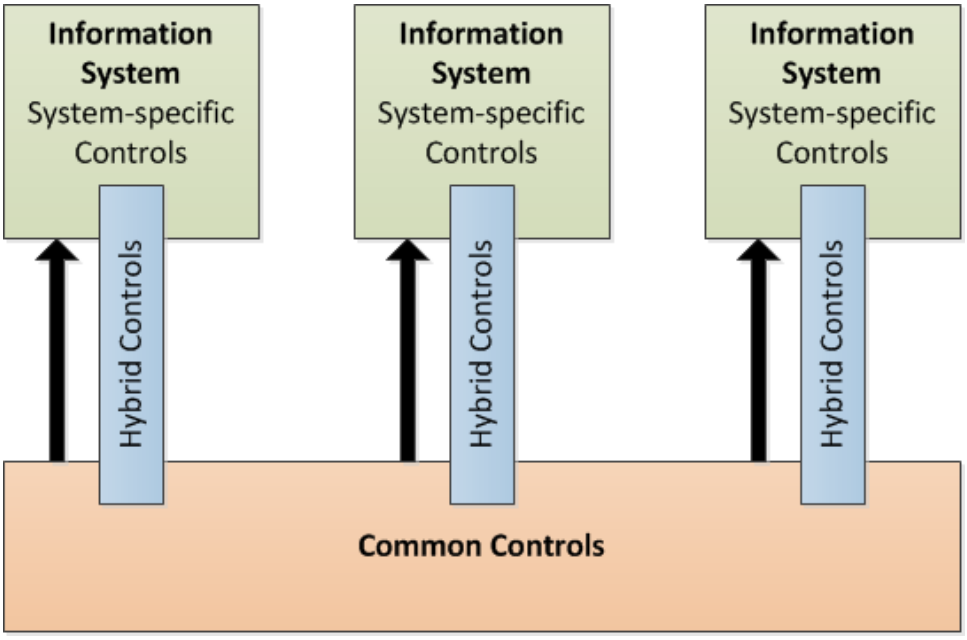
- One system was authorized to operate without a baseline of standard software that would be used within the system.

B. *Responsibility for implementing controls must be established in order to provide consistent, cost-effective security*

Since systems are often interconnected and interdependent, there must be a clear understanding of how security responsibilities and resources are shared. Security for multiple information systems may be provided by *system-specific, common,* or *hybrid* controls. System-specific controls provide capabilities for a particular information system only; for example, an application likely includes its own mechanisms for governing users' activities. Common controls provide protections for more than one system; for example, a facility may provide physical and environmental protections for multiple systems residing in it. Hybrid controls have both system-specific and common aspects; for example, audit and monitoring of an application system could include application-specific event logging, with monitoring performed by a separate network operations center.

Figure 1 illustrates the allocation of security controls within an organization. If organizations can determine ways to share resources to protect the system, then they can promote more cost-effective and consistent information security. The process of allocating security controls makes specific entities responsible and accountable for developing, implementing, assessing, authorizing, and monitoring those controls. The process should involve senior personnel throughout an organization and include authorizing officials, systems owners, information security officers, information security architects, chief information officers, and risk executives.

Figure 1. **Allocating Security Controls to Organizational IT Systems**



Source: OIG, adapted from NIST guidance

We determined that responsibility for implementing security controls was not properly allocated in 5 of the 10 systems we evaluated. Our findings suggest that organization-wide planning, as called for by the Risk Management Framework,[8] has not occurred to the extent necessary to ensure responsibility and accountability for security is properly assigned to specific organizational entities.

Examples:

- Two system security plans indicated that system-specific auditing and monitoring security controls, although planned, had not been implemented for an extended time (over 3 years and through two security authorizations). After we pointed out these issues, the systems' staff suggested that it would be more appropriate for other entities to provide the controls and the operating unit (responsible for both systems) would need to determine who should be responsible for auditing and monitoring the systems.

- One system security plan identified remote access controls as system-specific and "fully implemented." We found, however, that the system lacked the capabilities to implement the control, while some control elements were being provided by other systems. We also found that staff could use personal equipment to access the system remotely, in violation of the system's security requirements.

- One system was maintained by two IT contractors who failed to coordinate responsibility for implementing security controls within the system.

C. The intended applications of controls must be adequately described to enable the compliant implementation of controls

A necessary part of security planning is to determine how to meet specific security requirements—such as controlling access, monitoring for malicious activity, or limiting unnecessary services that can be exploited by an attacker. Security plans must describe each control's intended application, in context, with sufficient detail to enable compliance. In addition, sufficiently detailed descriptions of controls give assessors information they need to test the system's implemented security technologies.

Consistent with previous FISMA reviews, 7 of 10 systems' security plans lacked this information, which is also necessary to understand risk. Moreover, most of the systems involved had been through more than one authorization cycle, during which the security plans should have been extensively reviewed by security control assessors and others, updated by system owners, and approved by authorizing officials.

Examples:

- One system's security plan did not describe how controls were to be applied in its virtual server environment, and our technical assessment revealed that these security controls were not adequately implemented.

[8] See NIST SP 800-37 (cited in appendix A).

- One system was authorized to operate despite a security plan that failed to describe how it implemented authentication and access controls, configuration management, and auditing and monitoring. Because the system's Plan of Action and Milestones reported these missing control descriptions as IT security weaknesses (see finding below), key steps (selecting and implementing security controls) in the security authorization process were delayed and subverted.

- A system security plan did not describe implementation details for significant controls, instead reporting them as planned. In four key controls that were described, we found significant inaccuracies, as well as vulnerabilities, when comparing the security plan descriptions with the actual implementations.

Deficient security plans can expose systems to risk in the long term. One system's support staff, after experiencing large-scale turnover, admitted to inadequately understanding the system's specific requirements and working controls.

II. Deficiencies in Critical Controls Place the Department's Systems at Risk

We assessed the effectiveness of a subset of key security controls that (1) control access so that a system is less vulnerable to unauthorized activity, (2) establish, implement, and enforce secure configuration of components so that systems are hardened against attacks, (3) identify and fix security flaws before attackers can use them to compromise a system, and (4) detect and monitor for intrusions to lessen the impact of compromises. These controls not only act as the front-line defense against attacks, but also help minimize their effect.

During our assessment, we reviewed the systems' security documentation, interviewed system personnel, and conducted technical examinations of system components when appropriate. Security plans for six systems indicated that less than 50 percent of these key controls were implemented. Staff for one system at NOAA acknowledged that its documentation was inaccurate, no remediation plans were in place, and ongoing control assessments had ceased. In effect, the staff was not actively managing the system's security. Our assessment found that none of its key security controls were implemented. [9]

Our assessment also revealed:

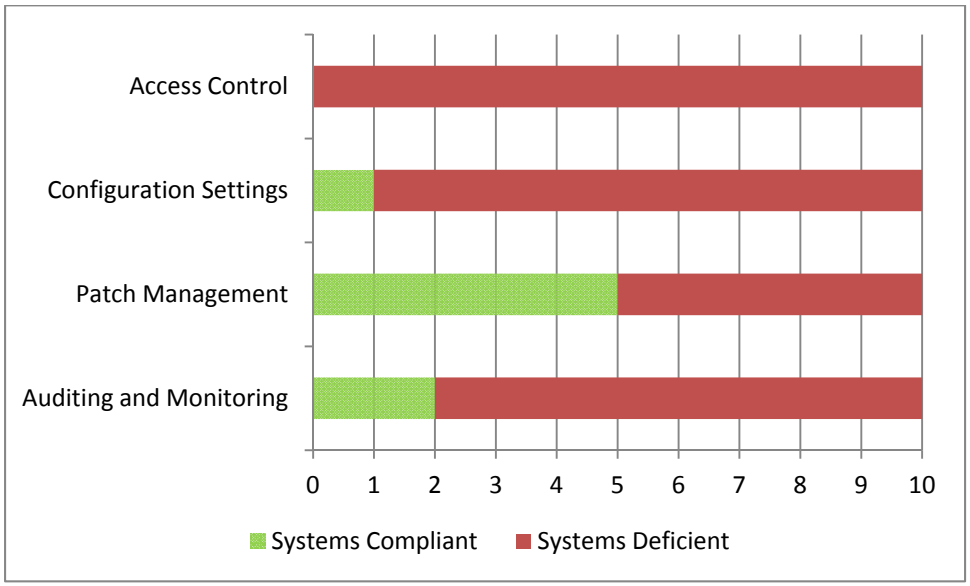
- Access controls were not adequately implemented in any of the 10 systems we assessed. In one case we found that system administrators, unlike system users, had unrestricted access to the Internet, and one administrator had inappropriately conducted personal business with a foreign-based company. After we informed the operating unit's management, it planned to augment content filtering and monitoring controls.

[9] This was the third system we have reviewed in the last 3 years where the security posture was essentially unknown, yet by authorizing the systems to operate, operating unit officials asserted an understanding and acceptance of risk. See *FY 2009 FISMA Assessment of the Environmental Satellite Processing Center* (OAE-19730) and *FY 2009 FISMA Assessment of BIS IT Infrastructure* (OSE-19574).

- Secure configuration settings were not adequately defined or implemented for one or more major IT products in 9 systems.
- Software patches for high-risk vulnerabilities were missing in 5 systems.[10]
- Auditable system events, which must be logged and are needed to support investigations of security incidents, were not defined for 7 systems. One additional system was not configured to log its required auditable events.

A summary of our security control assessment is presented in figure 2.

Figure 2: **Summary Assessment of Key Information System Security Controls**



Source: OIG

These key IT security controls are necessary for effective cyber defense. With deficiencies in these controls, the systems are more susceptible to attacks or other compromises of information confidentiality, integrity, and availability. Our findings were largely consistent with operating units' own control assessments (including those from continuous monitoring efforts), which identified numerous security weaknesses in 8 of the 10 systems.

[10] The Department has not yet completed actions in response to our recommendation, from our FY 2010 report, to improve vulnerability scanning and patch management policies to ensure comprehensive identification of vulnerabilities and timely remediation of software flaws.

III. Deficiencies in the Department's Plan of Action and Milestones (POA&M) Process Undermine Effective Remediation of Security Weaknesses

FISMA requires that the Department's information security program include a process for planning, implementing, evaluating, and documenting actions necessary to remediate security weaknesses. The Department's mechanism for reporting and tracking IT security weaknesses and corrective actions is the Plan of Action and Milestones (POA&M).

In our FY 2010 FISMA audit, we found significant deficiencies in the POA&M process that compromise the Department's ability to effectively track the status of corrective actions. Because POA&M metrics are used as performance measures, for people with significant IT security responsibilities, the lack of integrity controls in the process increases the risk that positive performance ratings may be inappropriately achieved. The Department concurred with our recommendation to revise and implement its POA&M policy to include integrity controls, evidence requirements, and management oversight, but has not yet completed the necessary revisions, which it targets for completion by December 2011.

In the meantime, we found deficiencies in FY 2011 similar to those we found in FY 2010. These include:

- IT security weaknesses that were not added to POA&Ms, leaving management without knowledge of system risk factors;
- POA&M-listed IT security weaknesses that were closed—indicating that a weakness had been remediated—when, in fact, the weaknesses had not been corrected; and
- remediation plans that lacked interim milestones needed for tracking the progress of mitigations, and little or no progress remediating weaknesses after extended periods (in some cases, over 3 years).

A system's POA&M is among three key documents—along with a system security plan and security assessment report—that officials use to make risk-based authorization decisions. Without a reliable POA&M process, POA&Ms cannot be counted on to provide an accurate account of remediation measures or a clear estimate of how long systems will be exposed to increased risk before vulnerabilities are reduced or eliminated. Further, these deficiencies corrupt performance measures that rely on POA&M statistics. We look forward to the Department completing its actions in response to our FY 2010 audit report in this area.

Recommendations

To make the Department's information security program and practices more effective, the Chief Information Officer should:

1. Complete actions planned in response to our FY 2010 FISMA audit recommendations, as quickly as possible.

2. Develop a security planning checklist, or other planning tool, to help system owners and authorizing officials complete and maintain comprehensive security plans.

3. Determine the feasibility of conducting independent reviews at key steps in the risk management framework to ensure greater rigor and consistency in the security authorization process within the Department's various operating units. Consideration should be given to creating independent review teams with representatives from different operating units to share best practices and promote consistent application of Department policy and NIST guidance.

Summary of Agency Comments and OIG Response

In his response to the draft report findings and recommendations, the Department's Chief Information Officer concurred and noted that he will work with the operating units to implement the recommendations.

Appendix A: Objective, Scope, and Methodology

Our audit objective was to assess the effectiveness of the Department's information security program and practices by determining whether (1) implemented controls adequately protect the Department's systems and information, and (2) continuous monitoring is keeping authorizing officials sufficiently informed about the operational status and effectiveness of security controls. This report describes key issues that require senior managers' attention. While we used examples from individual systems to illustrate issues, we did not identify the systems; aggregate results informed our assessment of the overall effectiveness of the Department's IT security program. We will submit a separate report to OMB, answering a full scope of security-related questions, in further accordance with FISMA requirements.

We selected a targeted set of 10 systems, which perform critical Department functions within three major bureaus:

- Census Bureau
- National Oceanic and Atmospheric Administration (NOAA)
  - NOAA's National Environmental Satellite, Data, and Information Service (NESDIS)
  - NOAA's Fisheries Service
  - NOAA's National Weather Service (NWS)
- U.S. Patent and Trademark Office (USPTO)

To assess the effectiveness of the Department's information security program and practices, we

- assessed a subset of security controls on information system components, conducting vulnerability scans and specifically tailored manual assessments;
- reviewed system-related artifacts, including policy and procedures, planning documents, and other material supporting the continuous monitoring process; and
- interviewed operating unit personnel, including system owners, IT security officers, administrators (network, system, database), and security control assessors.

We reviewed the Department's compliance with applicable provisions of law, regulation, and mandatory guidance, including

- the Federal Information Security Management Act of 2002
- IT Security Program Policy and Minimum Implementation Standards, U.S. Department of Commerce, introduced by the Chief Information Officer on March 9, 2009
- 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
  - 800-18, *Guide for Developing Security Plans for Information Technology Systems*
  - 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*
  - 800-37, Revision 1. *Guide for Applying the Risk Management Framework to Federal Information Systems*[11]
  - 800-53, *Recommended Security Controls for Federal Information Systems*
  - 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*
  - 800-70, *Security Configuration Checklists Program for IT Products*
  - 800-115, *Technical Guide to Information Security Testing and Assessment*

We conducted our field work from January to August 2011 at Commerce headquarters, various field offices, and contractor hosting facilities in the District of Columbia, Florida, Maryland, and Virginia.

We performed this audit under the authority of the Inspector General Act of 1978, as amended, and Department Organization Order 10-13, dated August 31, 2006. We conducted this audit 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.

[11] NIST revised SP 800-37 in February 2010, reframing its principles in accordance with its Risk Management Framework and changing the title of the guidance. In its FY 2011 FISMA reporting instructions, OMB required federal agencies to follow SP 800-37, Revision 1 for continuous monitoring. Where it has not otherwise been indicated, the most recent revision was consulted.

Appendix B: Agency Response

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

NOV 0 3 2011

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

THROUGH: Earl B. Neal
Director, Office of IT Security, Infrastructure and Technology

FROM: Simon Szykman
Chief Information Officer

SUBJECT: Department's Comments in Response to the FY 11 Draft Report *Federal Information Security Management Act Audit: More Work Needed to Strengthen IT Security Department-wide*

This memorandum serves as the Department's response to the Commerce Inspector General's FY 11 Draft Report *Federal Information Security Management Act Audit: More Work Needed to Strengthen IT Security Department-wide.*

The Department's Chief Information Officer (CIO) concurs with the findings and recommendations outlined within this report. We will work as a Department and collectively with the operating units to implement the recommendations.

The Department looks forward to receiving the Commerce Inspector General's final report. Please contact Tim Hurr, IT Security Compliance Officer, at (202) 482-4288, if you have any questions.

cc: Brian McGrath, Chief Information Officer, Census Bureau
Joseph Klimavicz, Chief Information Officer, NOAA
John Owens, Chief Information Officer, USPTO
Catrina Purvis, Chief Information Officer, NESDIS
Larry Tyminski, Chief Information Officer, NMFS
Iftikhar Jamil, Chief Information Officer, NWS