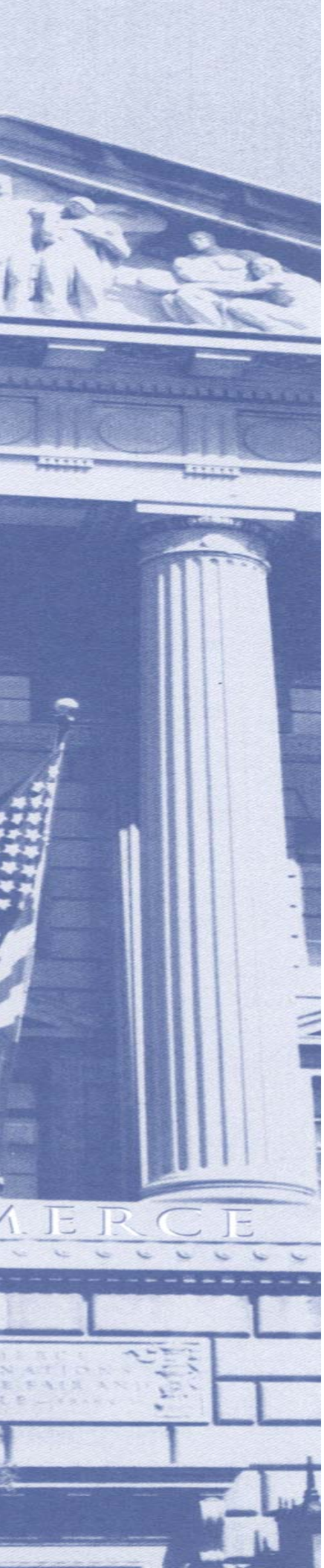

*U.S. DEPARTMENT OF COMMERCE*

*Office of Inspector General*

# *Office of the Secretary*

## *Federal Information Security Management Act Audit Identified Significant Issues Requiring Management Attention*

*Final Report OIG-11-012-A*

*November 15, 2010*

## *FOR PUBLIC RELEASE*

*Office of Audit and Evaluation*

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

November 15, 2010

**MEMORANDUM FOR:** The Honorable Gary Locke
The Secretary of Commerce

**FROM:** Todd J. Zinser

**SUBJECT:** Federal Information Security Management Act Audit Identified Significant Issues Requiring Management Attention
Final Report OIG-11-012-A

Under FISMA and Department policy, IT security is a shared responsibility of senior program officials and the Department's Chief Information Officer (CIO). While the Office of the Secretary is ultimately responsible for ensuring the security of the Department's information and information systems, senior officials must manage and supervise the IT security programs in their respective operating units.

IT security is one of the top management challenges identified by the Office of Inspector General. In previous years, we have issued system-level, detailed reports of FISMA evaluations to operating units, while also briefing the Department's CIO. In our FY 2010 FISMA audit, however, we analyzed aggregate results and focused on Department-wide deficiencies. The attached report presents the results of our audit, in which we assessed a targeted selection of 18 information systems from across the Department. We identified significant issues requiring management attention. Our four major findings were:

1. *Significant system vulnerabilities indicate the risk of a serious breach is greater than what was previously understood by operating units' management.* High-risk vulnerabilities stem from inadequate patch management and vulnerability scanning policy, procedures, and practices. Further, system components continue to be configured in a way that is not secure; secure configurations could limit the exploitation of software flaws.

2. *The Department's process for reporting and tracking security weaknesses is deficient.* We found significant deficiencies that affect the integrity of the information and compromise the Department's ability to effectively track the status of corrective actions, and which may also corrupt performance measurement.

3. *Contingency planning weaknesses threaten systems' ability to restore data and operations after disruption.* One third of the systems we reviewed did not test contingency plans in accordance with policy; five systems required to have alternate processing sites do not. We are particularly concerned about systems that support the Department's primary mission-essential functions.

4. *Persistent deficiencies in security plans and control assessments reduce the overall level of information assurance.* Consistent with previous reports, we continue to find security plan and control assessment deficiencies that prevent accurate assessments of risk.

In our report, we recommended that senior officials and the CIO revise the IT security policy by providing specific implementation guidance that will ensure more effective and consistent practices across the Department. Further, increased management attention is required to ensure that the deficiencies identified are rectified Department-wide. In his response to our draft report, the CIO concurred with our findings and recommendations.

We ask that you direct senior program officials and the CIO to submit an audit action plan to us by January 15, 2011. The plan should describe in detail the actions senior officials and the CIO are taking, or plan to take, in response to the specific recommendations made in the attached report.

If you would like to discuss any of the issues raised in the report, please call me at (202) 482-4661, or Allen Crawley, Assistant Inspector General for Systems Acquisition and IT Security, at (202) 482-1855.

Attachment

cc: Jay Reich, Senior Advisor and Deputy Chief of Staff
David Kappos, Under Secretary of Commerce for Intellectual Property and Director of the United States Patent and Trademark Office
Scott B. Quehl, Chief Financial Officer and Assistant Secretary for Administration
Simon Szykman, Chief Information Officer
Chief Information Officer's Council
Chief Financial Officer's Council
Susan Schultz Searcy, Audit Liaison, Office of the Chief Information Officer

# Report In Brief

U.S. Department of Commerce, Office of Inspector General

November 15, 2010


## Why We Did This Review

The Federal Information Security Management Act of 2002 (FISMA) requires agencies to secure their information systems, commensurate with the risk of loss or unauthorized use of system data. Inspectors general must annually evaluate agency information security programs by assessing a representative sample of such systems, and reporting the results to the Office of Management and Budget (OMB) and to Congress.

## Background

The Department and its operating units use over 300 information technology (IT) systems; this year we assessed security controls of 18 systems, from six different operating units.

Security weaknesses have been a long-standing problem for Commerce, particularly with respect to security planning, configuration settings, and control assessments. This year's review focused on Department-wide issues that require policy improvements and increased management attention.

## Office of the Secretary

## *Federal Information Security Management Act Audit Identified Significant Issues Requiring Management Attention* (OIG-11-012-A)

## What We Found

The Department's information security program and practices are not adequately securing Department systems, and we are concerned that the likelihood and severity of security breaches are considerably greater than what is currently perceived by management. The following table summarizes our major audit findings:

| Measure | Finding |
|---|---|
| ***High-risk vulnerabilities identified?*** | Extensive vulnerabilities in system software suggest considerable likelihood of a security breach; patch management and vulnerability scanning practices are not effective. Scans identified significantly more high-risk vulnerabilities than were previously known. |
| ***Configuration settings defined and documented?*** | Only 4 of 18 systems (one high-impact) adequately defined and documented secure settings for operating systems and major applications. This is a long-standing deficiency in a crucial security practice. |
| ***Configuration settings securely implemented?*** | Only one system securely configured settings for its operating systems. |
| ***Security weaknesses and corrective actions adequately reported and tracked?*** | Most systems exhibited significant deficiencies in reporting and tracking security weaknesses. As a result, the information about corrective action that the Department is using for performance measurement is inaccurate and inconsistent. |
| ***Contingency plans adequately tested?*** | Six of 18 systems' contingency plans were inadequately tested, including 2 systems that support the primary mission-essential weather forecasting function; testing of these 2 systems' contingency plans had not been done since FY 2007. |
| ***Alternate processing sites arranged?*** | Five systems that are required to have alternate processing sites do not have them, including three systems—two high-impact and one moderate-impact—that support weather forecasting. Documents attribute the lack of alternate sites primarily to budget constraints. |

## What We Recommend

We recommend that the Department revise its information security policy by providing specific implementation guidance that will ensure better and more consistent practices across the Department. Further, increased management attention is required to ensure that the deficiencies identified are rectified Department-wide.

# Contents

# Introduction

The Department of Commerce and its constituent operating units use over 300 information technology (IT) systems to fulfill cross-cutting responsibilities in trade, technology, entrepreneurship, economic development, environmental stewardship, and statistical research and analysis. These systems perform functions as varied as processing census and economic data, managing patent and trademark applications, and controlling weather satellites. The Department and its operating units must ensure that these systems maintain the confidentiality, integrity, and availability of information by providing protection from a growing range of malicious actors who can leverage the globally interconnected information and communications infrastructure to launch attacks. The systems must also be guarded against insider threats, physical intrusion, and disaster.

The Federal Information Security Management Act of 2002 (FISMA) requires agencies to secure systems through the use of cost-effective management, operational, and technical controls. The goal is to provide adequate security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information collected or maintained by or on behalf of an agency. In addition, FISMA requires inspectors general to evaluate agencies' information security programs and practices by assessing a representative subset of agency systems, and report the results to the Office of Management and Budget (OMB) and Congress annually.

We assessed information security controls and security-related documentation of 18 systems selected from six operating units, including three systems from the U.S. Patent and Trademark Office (USPTO), which files its own performance and accountability report separate from the Department. The operating units categorized these systems as high- or moderate-impact, based upon how severely a security breach would affect organizational operations, assets, or individuals.[1] Seven of the systems that we reviewed support three of the Department's four primary mission-essential functions, those that directly support government functions necessary to lead and sustain the nation during a catastrophic emergency.[2] This aspect of these systems adds importance to one focus of this report: contingency planning requirements necessary to minimize the impact of disruptions.

Details of our objectives, scope (including a complete list of systems reviewed), and methodology are described in appendix A.

### *IT Security Roles and Responsibilities*

Under FISMA and Department policy, IT security is a shared responsibility of senior program officials and the Chief Information Officer (CIO). While the Secretary of Commerce is ultimately responsible for ensuring the security of the Department's information and information

[1] See *Standards for Security Categorization of Federal Information and Information Systems*, Federal Information Processing Standards Publication 199, National Institute of Standards and Technology, February 2004.
[2] See U.S. Department of Commerce, "Emergency Readiness for Departmental Continuity," www.osec.doc.gov/omo/dmp/daos/dao210_1.html, accessed October 25, 2010.

systems, senior officials must manage and supervise the IT security programs in their respective operating units.

The CIO has a range of responsibilities, chief among them to develop and maintain the IT security policy; to designate a Chief Information Security Officer; and to monitor, evaluate, and report to the Secretary on the status of IT security within the Department. The Chief Information Security Officer directs the management of the Department's IT security program, a task that includes coordinating IT security compliance across operating units and developing policies, plans, control techniques, and procedures for systems.

Operating units have roles and responsibilities that parallel those at the Department level, with the operating unit head ultimately responsible for the security of the operating unit's systems. In addition, authorizing officials, who have the authority to oversee an information system's budget and operations, assume the responsibility for operating IT systems at an acceptable level of risk. Notably, authorizing officials also approve system security requirements and security plans. System owners must ensure that a system is deployed and operated in accordance with security requirements. System security officers ensure that operational security is appropriately maintained and play an active role in developing and updating system security plans. Certification agents independently assess a system's security controls, including an initial assessment of the security plan to determine whether the controls described adequately meet applicable security requirements.

### *Department Efforts to Improve IT Security*

In response to a September 2009 Office of Inspector General (OIG) audit of the Department's IT security workforce,[3] the Department established a policy, effective for all operating units, requiring mandatory training for those employees with significant IT security responsibilities. The policy identifies specific IT security roles, defines yearly minimum training hours, and requires professional certifications for those with critical IT security roles. The Department has also implemented a cyber security employee development program designed to assist individuals who have not earned an approved industry professional security certification. In FY 2010, 20 individuals became the first graduates of the program.

A key aspect of the IT security challenge is maintaining and enforcing effective IT security policies across the Department. Commerce operating units have separate management structures that preclude direct accountability of their CIOs to the Department's CIO. This decentralization gives the Department's CIO only limited authority to ensure operating units' compliance with IT security policy and adds complexity to Department-wide information security initiatives.

Notwithstanding this challenge, the CIO, along with the CIO Council, has developed a strategic plan that seeks "federated" approaches in two priority IT security initiatives: enterprise continuous monitoring and an enterprise security operations center. The plan is currently targeted for FY 2012. In this report, we identify deficiencies that require more immediate management attention.

[3] U.S. Department of Commerce, Office of Inspector General, September 2009. *Commerce Should Take Steps to Strengthen Its IT Security Workforce*, Report No. CAR-19569-1.

# Findings

Significant vulnerabilities exist in nearly all of the systems we selected for review. The scope of the vulnerabilities, categorized as high-risk, suggests that the likelihood and severity of a breach in the confidentiality, integrity, or availability of Department data are greater than what is currently understood by management. This previously unknown risk stems from inadequate vulnerability scanning, which has not sufficiently identified high-risk flaws, and poor patch management practices. In addition, we continue to find insecure configuration settings in system components.

The process for tracking vulnerabilities is deficient, and an inaccurate and inconsistent view of risk and remediation exists across the Department. Of further concern, contingency plans for 6 of the 18 systems reviewed have not been adequately tested. Five systems required to have alternate processing sites do not have them. As a result, the ability of these systems to adequately recover from a disruption—and some of these systems support primary mission-essential functions—is in doubt.

In addition, nearly all of the systems that we reviewed lacked security planning and effective assessment of security controls—conditions that we have consistently identified in previous years. Unless Department executives take action to appropriately mitigate and consistently manage risk, the Department's systems will remain unacceptably vulnerable to cyber attacks and other threats to information security.

## I. Significant Vulnerabilities in Commerce Information Systems Increase Risk of Serious Breach

Department policy—which, for "flaw remediation," is based entirely on the minimum security requirements for federal systems[4]—requires the organization to identify, report, and correct software flaws that result in potential security vulnerabilities. Newly released security patches, service packs, and "hotfixes" must be promptly installed, and flaws discovered during security assessments must be addressed expeditiously. Further, operating units are required to conduct vulnerability scanning (automated detection of software flaws and malicious code in system components) quarterly or when significant new vulnerabilities potentially affecting the system are identified and reported (for example, in a bulletin from a software manufacturer).

In addition, operating units must establish mandatory configuration settings (parameters that govern software's behavior) for information technology products, configure security settings to their most restrictive mode, document the settings, and enforce them in all components of the information system. Operating units must also assess configuration settings of IT products at least annually. Settings not securely configured represent potential vulnerabilities and pose risks similar to those of software flaws.

[4] Flaw remediation is required control SI-2 in *Recommended Security Controls for Federal Information Systems*, Special Publication 800-53, Revision 2, National Institute of Standards and Technology, December 2007.

To validate the extent to which these requirements are met across the Department, we analyzed the results of network vulnerability scans performed on 14 systems.[5] We assessed the extent to which secure configuration settings were established on all 18 systems by reviewing system documentation and examining settings implemented in components using automated and manual methods.

### *A. System Components Operate with Many Significant Software Flaws*

Vulnerability scans of 1,063 computers in 14 systems revealed a total of 13,778 instances of potentially high-risk vulnerabilities; 11 non-USPTO systems (1,003 computers) accounted for 12,626 of the vulnerabilities and 3 USPTO systems (60 computers) had a total of 1,152 vulnerabilities.[6] We performed 12 of the system scans and utilized the results of 2 system scans that the National Oceanographic and Atmospheric Administration (NOAA) adequately executed during our fieldwork. We have shared system-specific results with the operating units, and they are currently taking corrective action to remediate the vulnerabilities identified.

These vulnerabilities may provide an attacker with immediate access into a computer system, such as allowing remote execution of malicious commands. Vulnerabilities identified by the scans may be exploited by software tools freely available on the Internet. The flaws exist in both operating systems and application software.

Factors contributing to the existence of extensive software flaws include insufficient flaw remediation and vulnerability scanning policy, procedures, and practices. Risk can be reduced by timely remediation of flaws, often referred to as effective patch management. The large number of instances of vulnerabilities indicates that operating units are not promptly installing patches and other software fixes. In fact, we found instances of flawed software where the patches to fix the vulnerabilities had been available from the manufacturer for up to 5 years.

Although Department policy is in compliance with the minimum requirements set by National Institute of Standards and Technology (NIST), it does not adequately reduce vulnerabilities. This is due, in part, to the lack of provisions for senior management to ensure that flaw remediation is adequately performed. Our review of system documentation revealed that 11 of the 18 systems either had deficient patch management practices, or they were considered a "planned control" (meaning that the systems did not currently have complete patch management procedures, but system owners planned to develop and implement them at some point in the future). This security control is critical to ensuring that systems are adequately protected.

Beyond requiring operating units to scan on a quarterly basis, Department policy includes no specifications for the depth and breadth of scanning. For example, no requirement exists for the use of credentialed scans, which utilize administrator-level, privileged access to allow a scanning tool to perform a more exhaustive and accurate examination of a system. The policy also leaves uncertain what vulnerability checks a scanner must employ. As we found, this has resulted in inconsistent practices across the Department.

[5] See appendix A, *Objectives, Scope, and Methodology*, for details of our vulnerability scan assessment.
[6] The vulnerabilities identified may include false-positives, which potentially include conditions not accurately reported by the scanners. However, our scanning practices, which include the use of administrator-level credentials, tend to minimize the number of false positives.

Some operating units either were not performing credentialed scans or had only recently begun credentialed scanning. One operating unit's quarterly scanning focused on a very limited set of the top 20 vulnerabilities identified by a private security organization. As tables 1 and 2 illustrate, more thorough scanning, to include credentials and sufficient vulnerability checks, is necessary to ensure that software flaws are sufficiently identified.

We compared our non-USPTO assessment results with operating units' most recent quarterly scans and included both in table 1. On average, we identified over 3 times as many high-risk vulnerabilities per computer than were identified by the operating units' quarterly scans. The scans for our assessment identified 4.2 vulnerabilities per computer, compared with 1.3 per computer identified by the operating units' quarterly scans of the same systems, after adjusting for one NOAA system that was a statistical outlier. This NOAA system accounted for 9,299 instances (74 percent) of the vulnerabilities, although NOAA has since made progress by installing patches that have significantly reduced this number.

### *Table 1. Comparison of Vulnerability Scans Conducted on Selected Non-USPTO Systems*

| Basis for Scan | Systems Scanned | Computers Scanned | High-Risk Vulnerabilities | Vulnerabilities per Computer[a] |
|---|---|---|---|---|
| Operating Unit Quarterly | 10 | 1,427 | 1,842 | 1.3 |
| (including outlier system) | (11) | (1,509) | (1,916) | (1.3) |
| OIG FISMA Audit | 10 | 784 | 3,327 | 4.2 |
| (including outlier system) | (11) | (1,003) | (12,626) | (12.6) |

[a] High-Risk Vulnerabilities / Computers Scanned

Source: OIG and operating unit scans

Findings from our vulnerability assessment for three USPTO systems are presented in table 2. Particularly for the two systems in our subset operated by USPTO, our scans identified many more vulnerabilities per computer than USPTO's annual scan (30.5 versus 1.7). USPTO did not perform quarterly scanning of these two systems, as mandated by policy. The third USPTO system, operated by a contractor, was scanned quarterly. The contractor's quarterly scans were comprehensive, identifying the same number of high-risk vulnerabilities per computer (14.7) as our audit scan.

### *Table 2. Comparison of Vulnerability Scans Conducted on Selected USPTO Systems*

| Basis for Scan | Systems Scanned | Computers Scanned | High-Risk Vulnerabilities | Vulnerabilities per Computer[a] |
|---|---|---|---|---|
| USPTO Quarterly | 2 | 322 | 537 | 1.7 |
| (including contractor system) | (3) | (1,503) | (17,856) | (11.9) |
| OIG FISMA Audit | 2 | 17 | 518 | 30.5 |
| (including contractor system) | (3) | (60) | (1,152) | (19.2) |

[a] High-Risk Vulnerabilities / Computers Scanned

Source: OIG and USPTO scans

### *B. Information Technology Systems Are Not Securely Configured, Reducing Their Ability to Withstand Attack*

Secure configuration checklists, which document tailored security settings for IT products, were not adequately defined in 14 of the 18 systems. We reviewed documentation for operating systems and major applications (such as database management systems, Web servers, and domain name servers); only four systems had adequately defined secure configuration checklists.

In addition, we assessed actual operating system and database (where applicable) configuration settings implemented in system components by comparing them against either the system's tailored checklist or, if no tailored checklist existed, an industry benchmark. Only one system had securely configured settings implemented for its operating systems (it did not include databases). (See table 3.)

## *Table 3. Compliance With Configuration Settings Requirements*

| System Categorization | Systems Assessed | Systems with Defined Checklists | Systems with Secure Settings[a] |
|---|---|---|---|
| High Impact | 6 | 1 | 0 |
| Moderate Impact | 12 | 3 | 1 |
| ***Total*** | ***18*** | ***4*** | ***1*** |

[a] We did not assess the implemented settings in one NOAA system due to concerns about its high-availability operational requirements during hurricane season.

Source: OIG

Department systems are not in compliance with requirements for configuration settings—requirements important enough that we must report to OMB separately on them each year. Securely configured settings have the potential to compensate for other types of vulnerabilities and can limit the impact of cyber attacks. We have consistently reported on configuration settings deficiencies in our annual FISMA work. These recurring findings suggest the need for increased management attention and improved policy at the Department level.

Current policy requires specific configurations for workstations running Windows® operating systems, in accordance with a federal mandate.[7] However, no specific configurations are required for server operating systems or other software, despite the public availability of a variety of specific configurations. Rather, operating units are required to define specific configurations, starting with an industry benchmark of their choosing, and then tailor it to define a specific checklist of settings. However, our reviews have consistently found that operating units are deficient in meeting this requirement.

[7] The Federal Desktop Core Configuration (FDCC) is an OMB-mandated security configuration. The FDCC currently exists for Microsoft Windows Vista® and Windows XP® operating system software.

## II. Departmental Process for Reporting and Tracking IT Security Weaknesses and Corrective Action Is Deficient

FISMA requires that the Department's information security program include a process for planning, implementing, evaluating, and documenting action necessary to remedy security weaknesses, including vulnerabilities identified in control assessments.

The Department's mechanism for reporting and tracking IT security weaknesses and corrective action is the Plan of Action and Milestones (POA&M), as required by OMB. For the past 2 fiscal years, the Department has required operating units to manage POA&Ms using its Cyber Security Assessment and Management tool (CSAM).[8] The Department is required to submit a quarterly report to OMB with summary POA&M information. However, we found significant deficiencies in the POA&M process that affect the integrity of the information and compromise the Department's ability to effectively track the status of corrective action.

### *A. Plans of Action and Milestones Lack Information Needed for Tracking and Oversight*

Senior management, including the Department's CIO, is not informed of or providing oversight to system-level vulnerabilities as required because known security weaknesses are not entered in system POA&Ms. Likewise, the Department's summary report to OMB is understating the number of security weaknesses in Department systems. Eleven systems we reviewed included evidence of deficient security controls that are not included in the systems' POA&Ms. In some cases, system security plans indicated that required security controls are "planned" (not implemented), but the absence of the controls and plans to implement them are not reported in the POA&M.

In addition, incomplete information hinders management's ability to effectively monitor the scope of security weaknesses and measure actual progress toward correcting them. Eleven of the 18 systems' POA&Ms exhibited one or more of the following conditions:

- POA&M-listed weaknesses were "closed" (an assertion that the vulnerability had been remediated) without supporting evidence or even an indication of what corrective action had been taken.

- Descriptions of security weaknesses were so vague that it was unclear what actually needed to be corrected. For example, one weakness was described as "Improving the C&A Package 800-53:RA-05 Vulnerability Scanning." No additional details or milestone activities were provided, leaving the measurement of what was to be done (improve documentation? policies? practices?) and how (types of components? time interval?) unspecified.

- Planning elements such as milestones for remediation activities were omitted or contradictory. For example, a weakness that was targeted for remediation in 2015 had just two milestones—both in 2011, leaving a 4-year gap between the last corrective activity and the planned completion date.

[8] CSAM is a Web-based application that provides a common interface and repository of information.

### *B. Reporting and Tracking Process Lacks Controls over Data Integrity*

Inconsistency in the POA&M process prevents management from having an accurate account of security weaknesses and plans to correct them. New in fiscal year (FY) 2010, the departmental CIO, along with the Director of Human Resources, instituted an individual performance metric for key system staff that measures the extent to which POA&M items are closed (weaknesses corrected) on schedule. Without policy requirements for scheduling corrective action, closing POA&M-listed weaknesses, and a separation of roles in the POA&M process, a single individual may have the ability to falsely improve his/her performance rating or that of the organization. Fourteen of the 18 systems we reviewed exhibited evidence of one or more of the following:

- *POA&M items were closed but security weaknesses were not corrected.* An egregious example of this was a high-impact system for which all 191 items on its POA&M were closed in the first quarter of FY 2010 based on an assertion that the system's security controls would be reassessed within 6 months. However, the reassessment has been postponed—it is currently planned for the third quarter of FY 2011—while the weaknesses persist, unreported and unmanaged.

- *Old POA&M items were closed and reopened as new items, inaccurately reporting the timeliness of corrective action.* As a planned date for completion of corrective action approached (or in some cases, after it became due), IT security personnel canceled or closed the POA&M item and added a new item to the POA&M for the same weakness, with a corresponding new planned completion date farther into the future.

- *Planned completion dates were excessive for relatively simple actions required to remediate weaknesses.* For example, a lack of passwords required for administrator accounts was reported on one system's POA&M in May 2009; the scheduled completion date for correcting the deficiency was in June 2010. Over 1 year was deemed an appropriate time frame for resolving a critical yet basic security control.

- *There was no "separation of duties"—necessary to ensure the integrity of the process.* The person requesting closure of the POA&M item (the individual asserting that the weakness has been corrected) was the same person later authorizing the closing of the item (*verifying* evidence of the corrective action). While some operating units do utilize separate roles in the closure process, this is not consistent Department-wide, and current policy does not address this issue.

The Department's current policy for POA&Ms addresses what types of security deficiencies must be included, instructions for various fields in the POA&M form, and operating units' quarterly reporting requirements that have since been superseded by the reporting capabilities of CSAM. The policy does not address standards of evidence for closing deficiencies listed on POA&Ms or a role structure to ensure separation of duties with respect to the process. Improved policy and consistency in its application across the Department are needed to ensure that accurate data are available to senior management and in reports to OMB.

## III. Contingency Planning Weaknesses Threaten Operating Units' Ability to Restore System Data and Operations After Disruption

Contingency planning controls are intended to ensure the capability to quickly and competently recover from a variety of disruptions, minimizing the loss of availability and preserving the integrity of data. Department policy, in accordance with minimum requirements for federal systems, requires operating units to test contingency plans at least annually to determine their effectiveness and the organization's readiness to execute them.

The policy also requires moderate- and high-impact systems to have alternate processing sites that allow critical functions to resume when primary processing capabilities are disrupted. An alternate processing site must be geographically separated from the primary processing site in order to prevent both from being susceptible to the same local environmental hazards and disasters. High-impact systems' alternate processing sites must be tested to ensure that capabilities to support contingency operations are in place.

Contingency planning also contributes to continuity of operations in support of the Department's Primary Mission-Essential Functions—departmental functions that directly support National Essential Functions (government functions necessary to lead and sustain the nation during a catastrophic emergency). The Department has four such essential functions, in the following areas: (1) export control, (2) environmental satellites, (3) weather forecasting, and (4) spectrum management and the Internet. Of the systems we reviewed, one Bureau of Industry and Security system supports the export control-related function and six NOAA systems support the satellite- or weather forecasting-related functions.

For the past 2 years, our FISMA reviews have identified instances in which contingency plans were tested insufficiently or not at all. While the Department has made progress,[9] our review indicated that these same weaknesses, which undermine the Department's ability to restore operations in a timely manner when serious disruption occurs, are continuing.

### *A. Contingency Plans Are Not Adequately Tested*

Of the 18 systems we reviewed, 6 were not tested in accordance with Department policy (see table 4.). Three high-impact systems and one moderate-impact system were not tested annually as required, including two NOAA systems that had not been tested since FY 2007; both of those systems support the primary mission-essential weather forecasting function. National Weather Service personnel currently responsible for the systems explained that they received ownership of the systems from the weather service's Office of the Chief Information Officer in the second quarter of FY 2010, and that the contingency plans will be tested in FY 2011.

Two systems' contingency plan tests were inadequate: one high-impact system's test did not comply with policy requirements in that it lacked an alternate processing site at which to conduct testing. And a business continuity/disaster recovery test was conducted on one moderate-impact system, but the test did not validate the recovery and restoration procedures described in the contingency plan.

[9] In FY 2008, 44 percent of the contingency plans we reviewed were tested in accordance with Department policy; in FY 2009, 50 percent were adequately tested; in FY 2010, 67 percent were adequately tested.

### *Table 4. Summary of Contingency Plan Testing*

| System Impact Level | Systems Reviewed | *Contingency Plans* | | |
|---|---|---|---|---|
| | | Adequately Tested | Not Tested | Inadequately Tested |
| High | 6 | 2 | 3 | 1 |
| Moderate | 12 | 10 | 1 | 1 |
| ***Total*** | ***18*** | ***12*** | ***4*** | ***2*** |

Source: OIG

Testing informs and affects other required contingency planning activities and controls; the lack of contingency plan testing could have a ripple effect on operating units' ability to respond and recover in the event of a system failure, emergency, or other disruption. Such other elements include updating the plan based on lessons learned in the testing, conducting annual refresher contingency training of personnel, testing backup information, and (for high-impact systems) testing full recovery and reconstitution procedures. All of these actions are part of the minimum requirements for preparing for emergency response, backup operations, and post-disaster recovery.

In the case of three systems whose contingency plans were tested, the depth and rigor of testing performed may no longer be considered sufficient under recently revised NIST guidance for contingency planning.[10] Three moderate-impact systems' contingency plan tests were "tabletop," rather than "functional," exercises.[11] The revised guidance indicates that functional exercises should be conducted for moderate- and high-impact systems, while tabletop exercises are sufficient for low-impact systems only. Department policy requires operating units to follow this guidance for contingency planning, but does not refer to the guidance in its contingency plan testing and exercises requirements. The policy requires that the depth and rigor of testing increase with the system's impact level, but does not provide concrete examples.

### *B. Systems Lack Alternate Processing Sites, Increasing the Risk of Not Being Available When Needed*

Five systems that are required to have alternate processing sites do not, including three NOAA systems (of which two have high-availability requirements) that support the weather forecasting primary mission-essential function. NOAA has plans to arrange alternate processing sites by the end of 2011 and 2015, respectively, for the two high-availability systems. The third NOAA system's documentation indicates that the lack of an alternate processing site is an accepted risk; the system is scheduled to be decommissioned by the end of 2011. Planning documentation for

[10] National Institute of Standards and Technology. May 2010. *Contingency Planning Guide for Federal Information Systems* (NIST SP 800-34, Revision 1).

[11] According to NIST SP 800-34, *tabletop* exercises are discussion-based, in which personnel meet in a classroom setting to discuss their roles during an emergency and their responses to a particular situation. *Functional* exercises allow personnel to validate their operational readiness for emergencies by performing their duties in a simulated operational environment.

the NOAA systems indicates that the lack of alternate processing sites is due to "budget constraint and technical complexity" or other funding issues. However, the systems' plans of action and milestones do not include cost estimates for resolving these deficiencies. Two moderate-impact USPTO systems are subject to the operating unit's plan to arrange alternate processing sites for all its systems in a phased approach that will be completed in 2015.

Particularly for systems supporting primary mission-essential functions, the lack of alternate processing sites may pose undue risk of prolonged disruption to systems that are critical to ensuring continuity of essential governmental operations. High-availability systems that support weather forecasting and lack alternate processing sites imperil NOAA's ability to continually meet its goals of saving lives, protecting property, and creating economic opportunity. Based on our interviews with NOAA personnel and reviews of the systems' contingency planning documentation, events leading to a loss of the availability of the systems' primary processing sites would have dire consequences for the weather forecasting-related function.

## IV. Persistent Deficiencies in Security Plans and Control Assessments Reduce Overall Level of Information Assurance

Consistent with many of our previous FISMA reviews, system security plans lacked information necessary to adequately describe system-specific control requirements and implementations—information that senior officials need to assess risk. Security control assessments—which provide assurance that controls are adequately implemented, operating as intended, and providing the resulting security that systems require—depend upon clearly-defined requirements and adequately described implementations in order to accurately judge the effectiveness of security controls in the appropriate technologies. Thirteen of 18 systems' security plans lacked system-specific requirements or implementation details for security controls.

In addition, control assessments for 14 of 18 systems did not provide needed assurance; for example, some assessments of controls implemented in system components consisted of reviews of policy and procedures or interviews of staff, rather than technical examinations to validate components' configurations or tests to determine whether controls were operating correctly. In other cases, controls were assessed for only one type of component rather than what are often several (sometimes many) component types in which controls are implemented.

While we have previously reported these issues to operating units, often for individual systems and in great detail, and made the Department's Office of the Chief Information Officer aware, these deficiencies continue to exist to an extent that causes concern. The Department's efforts, in response to our IT security workforce audit,[12] to increase the knowledge and skills of personnel with IT security responsibilities should eventually result in improvements in these areas. However, it is not clear that senior officials are sufficiently aware of what have been longstanding problems that require more urgent attention.

[12] Commerce OIG, *Commerce Should Take Steps to Strengthen Its IT Security Workforce*.

# Recommendations

To improve the effectiveness of the Commerce information technology security program and practices, we recommend that senior officials with interim responsibility for the Deputy Secretary position ensure that the Chief Information Officer and senior management of the operating units work together to:

1. Revise the departmental information technology security policy by providing specific implementation requirements that will ensure better and more consistent practices across the Department. Specifically,

    a. improve vulnerability scanning and patch management policies to ensure comprehensive identification of vulnerabilities and timely remediation of software flaws;

    b. add specific configuration- settings requirements for operating systems, major applications, and other products; and

    c. clarify requirements for the depth and rigor of contingency plan testing.

2. Ensure that operating units take corrective action as necessary in response to our vulnerability scan assessments;

3. Increase Department and operating unit management oversight of vulnerability scanning and patch management so that software flaws are comprehensively identified and remediated in a timely manner;

4. Increase Department and operating unit management oversight of configuration settings to ensure that secure settings are defined, documented, and implemented for operating systems, major applications, and other products, as required;

5. Revise and implement POA&M policy to include integrity controls (including separation of duties), evidence requirements, and management oversight;

6. Ensure that operating units conduct contingency plan tests as required;

7. Identify all systems without required alternate processing sites and determine the most efficient approach, resources required, and a schedule for arranging sites; and

8. Ensure that system security plans adequately describe security controls and that control assessments provide needed assurance.

# Summary of Department Response

In responding to our draft report, the Department's Chief Information Officer concurred with our findings and recommendations. See appendix B for the complete response.

# Appendix A: Objectives, Scope, and Methodology

In accordance with FISMA, our objective was to assess the effectiveness of the Department's information security program and practices. This report describes key issues that most require senior management's attention. In general, we do not detail our findings for the individual systems reviewed unless such is necessary for clarity. We focused on aggregate results to assess 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.

Our assessment focused on a targeted selection of 18 systems from the following departmental operating units/sub-units:

- Bureau of Industry and Security (BIS)
- U.S. Census Bureau
- Economic Development Administration (EDA)
- National Oceanic and Atmospheric Administration (NOAA)
    - NOAA's National Environmental Satellite, Data, and Information Service (NESDIS)
    - NOAA's National Weather Service (NWS)
    - NOAA's National Ocean Service (NOS)
    - NOAA's Office of the Chief Information Officer (OCIO)
- Office of the Secretary (OS)
- U.S. Patent and Trademark Office (USPTO)

We selected high- and moderate-impact systems, some of which support primary mission-essential functions, because security breaches of these systems would have the greatest negative impact on the confidentiality, integrity, or availability of data and Department operations. (See table 5.)

To complete our assessment, we reviewed systems' security-related documentation, including system security plans, configuration settings checklists, Plans of Action and Milestones, security control assessments, and quarterly vulnerability scans. We performed our own vulnerability scans of 12 systems and assessed configuration settings in all 18. We utilized two NOAA system vulnerability scans that were adequately performed, during our fieldwork, by a NOAA unit newly responsible for the systems. We did not conduct vulnerability scanning of three Census systems due to concerns that our work might disrupt 2010 decennial census operations. Our vulnerability assessment of BIS's Investigative Management System Redesign was limited to configuration settings-related activities because vulnerability scanning was not appropriate for the technical composition of the system.

We performed our audit work from June to October 2010 at Commerce headquarters in Washington, D.C., and various Census, NOAA, and USPTO facilities in Maryland and Virginia.

We conducted our 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.

### *Table 5. Systems Reviewed*

| Operating Unit/Sub-unit | Impact Level | Supports Primary Mission-Essential Function |
|---|---|---|
| BIS | High | X |
| Census | Moderate | |
| Census | Moderate | |
| Census | Moderate | |
| EDA | Moderate | |
| NOAA | High | X |
| NOAA | Moderate | |
| NOS | Moderate | |
| NESDIS | High | X |
| NESDIS | High | X |
| NESDIS | Moderate | |
| NWS | High | X |
| NWS | High | X |
| NWS | Moderate | X |
| OS | Moderate | |
| USPTO | Moderate | |
| USPTO | Moderate | |
| USPTO | Moderate | |

Source: Department of Commerce

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

- Federal Information Security Management Act of 2002
- *IT Security Program Policy and Minimum Implementation Standards*, U.S. Department of Commerce, introduced by the CIO 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*
  - 800-34, *Contingency Planning Guide for Federal Information Systems*
  - 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*
  - 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*

# Appendix B: Full Text of Department Response

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

NOV 0 9 2010

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

THRU: Earl B. Neal
Director, IT Security, Infrastructure and Technology

FROM: Simon Szykman
Chief Information Officer

SUBJECT: Department's Response to the Draft FY10 *Federal Information Security Management Act Audit*

This memorandum serves as the Department's response to the Commerce Inspector General's Draft FY10 *Federal Information Security Management Act (FISMA) Audit.* The Department's Chief Information Officer (CIO) concurs with findings and recommendations outlined within this report.

The Department looks forward to receiving the Commerce's Inspector General's final audit report.

If you need further assistance or have any questions, please contact Tim Hurr at (202) 482-4822.

cc: David Kappos, Under Secretary of Commerce for Intellectual Property and Director of the United States Patent and Trademark Office (USPTO)
Scott B. Quehl, Chief Financial Officer and Assistant Secretary for Administration
Chief Information Officer's Council
Chief Financial Officer's Council

(OAE-19904)