



NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

Significant IT Security Program Improvements Are Needed to Adequately Secure NTIA's Systems

FINAL REPORT NO. OIG-12-035-A
SEPTEMBER 7, 2012

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

September 7, 2012

MEMORANDUM FOR: Lawrence E. Strickling
Assistant Secretary for Communications and Information
National Telecommunications and Information Administration

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

SUBJECT: FY 2012 Federal Information Security Management Act Audit:
*Significant IT Security Program Improvements Are Needed to
Adequately Secure NTIA's Systems, Final Report No. OIG-12-035-A*

Attached is the final report of our audit of NTIA's information security program and practices, which we conducted to meet our obligations under the Federal Information Security Management Act (FISMA). In FY 2012, we assessed the security of seven NTIA systems.

We found deficiencies in NTIA's systems, including (1) inadequate security categorizations that jeopardize critical bureau information, (2) significant weaknesses in IT software and hardware inventory practices, (3) major deficiencies in NTIA's security weakness remediation process, (4) weaknesses in managing its IT security workforce and developing effective IT security policies and procedures, and (5) significant deficiencies in key IT security controls.

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 OIG's website.

In accordance with Department Administrative Order 213-5, please provide us with your action plan within 60 calendar days from the date of this memorandum. 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 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: Simon Szykman, Chief Information Officer
Griff Drew, Chief Information Officer, NTIA
Tim Hurr, Acting Director, Office of Cyber Security
Milton Brown, Audit Liaison, NTIA
Susan Schultz Searcy, Audit Liaison, Office of the Chief Information Officer



Report In Brief

SEPTEMBER 7, 2012

Background

NTIA is principally responsible for advising the President on telecommunications and information policy issues. These issues include expanding broadband Internet access and adoption in America, ensuring that the Internet remains an engine for continued innovation and economic growth, managing the federal government's use of spectrum (airwaves), and ensuring that America's domestic and international spectrum needs are met while making efficient use of this limited spectrum resource.

Why We Did This Review

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 extent 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 the results are reported to the Office of Management and Budget, the Department of Homeland Security, and Congress annually.

NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

Significant IT Security Program Improvements Are Needed to Adequately Secure NTIA's Systems

OIG-12-035-A

WHAT WE FOUND

Fundamental steps for securing NTIA's information and systems have not been taken. When assessing seven NTIA systems, we found these deficiencies: (1) inadequate security categorizations that jeopardize critical bureau information, (2) significant weaknesses in IT software and hardware inventory practices, (3) major inadequacies in NTIA's process to remediate security weaknesses, (4) weaknesses in managing its IT security workforce and developing effective IT security policies and procedures, and (5) significant deficiencies in key IT security controls. These issues have resulted in ineffective management of security controls needed to protect NTIA's systems and information.

WHAT WE RECOMMEND

The Assistant Secretary for Communications and Information should ensure:

1. The authorization status of NTIA's systems is revised to interim authorization to operate until these activities have been completed:
 - a. System owners and NTIA officials collaborate to identify and categorize all information types that are processed, stored, or transmitted by each system and categorize each system accordingly.
 - b. System owners develop and maintain an accurate hardware and software inventory for their systems.
 - c. NTIA implements and assesses appropriate IT security controls.
 - d. NTIA follows the plan of action and milestones process required by the Department's IT security policy.
2. System owners, IT security officers, authorizing officials, and other staff with critical IT security roles are appropriately trained, earn certifications as required by Department policy, and have the required metrics incorporated into their performance plans.
3. NTIA's chief information officer and IT security officer develop and maintain NTIA security policies, procedures, standards, and guidance consistent with departmental and federal requirements.

Contents

Introduction	1
Findings and Recommendations	2
I. Inadequate Security Categorization Analysis Jeopardizes Critical Bureau Information	2
II. An Accurate Inventory of All Hardware and Software Components Is Essential for Ensuring Adequate System Security.....	3
III. Deficiencies in NTIA’s Plan of Action and Milestones Process Undermine Effective Remediation of Security Weaknesses	4
IV. Inadequate IT Security Workforce Management and Lack of IT Security Policies Adversely Affect NTIA’s IT Security Program	5
V. Significant Deficiencies in Key Security Areas Increase NTIA’s Exposure to Cyber Attacks.....	7
Conclusion	10
Recommendations	11
Summary of Agency Response and OIG Comments.....	12
Appendix A: Objective, Scope, and Methodology.....	13
Appendix B: Agency Response	15

Introduction

The Internet, spectrum frequencies, and telecommunications are some of the world's most valuable resources in the information age. NTIA is principally responsible for advising the President on telecommunications and information policy issues, such as expanding broadband Internet access and adoption in America, ensuring that the Internet remains an engine for continued innovation and economic growth, managing the federal government's use of spectrum, and ensuring that America's domestic and international spectrum needs are met while making efficient use of this limited spectrum resource.

The Federal Information Security Management Act of 2002 (FISMA)¹ 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 extent 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 the results are reported to the Office of Management and Budget, the Department of Homeland Security, and Congress annually.

As part of an overall assessment of the Department's information technology (IT) security program, we evaluated information security controls and security-related documentation for seven operational NTIA systems to determine whether key security measures adequately protect NTIA's systems and information. See appendix A for details regarding our objective, scope, and methodology.

¹ Federal Information Security Management Act of 2002, 44 U.S.C. § 3541 (2002).

Findings and Recommendations

As part of our FY 2012 FISMA work, we reviewed NTIA's IT security program and found that fundamental steps for securing NTIA's information and systems have not been taken. Additionally, the Department's process for remediating vulnerabilities and informing management of risks has not been effectively implemented. This has resulted in ineffective management of security controls needed to protect NTIA's systems and information.

I. Inadequate Security Categorization Analysis Jeopardizes Critical Bureau Information

NTIA's information systems lack sufficient IT security controls because the required step of identifying the critical information in the systems has not been properly performed. Without understanding the types of information that a system processes, stores, or transmits, an organization cannot make an accurate determination of the risks to the system and select appropriate security controls. The process used to make this determination is referred to as security categorization.² Security categorization identifies the impact level for a system as high, moderate, or low based on the potential impact to an organization, should an event jeopardize its information and information systems.

We found that five NTIA systems were miscategorized and should have been categorized at a higher impact level. NTIA systems categorized as low should be moderate or systems categorized as moderate should be high because NTIA did not identify all information types in its systems. For example we found that NTIA systems have information that (1) supports U.S. negotiators and interagency delegations in strategic international forums, (2) is used to advise elected officials and federal agencies in policy development, (3) includes proprietary commercial data, (4) supports law enforcement activities, or (5) supports the protection of elected officials. However, these information types were not identified in NTIA's security categorization process.

Because security categorization is a foundational step in the risk management process,³ NTIA's inadequate categorization analysis adversely affects all other IT security activities, including selecting and implementing appropriate security control baselines, applying the appropriate rigor to control assessments, and monitoring security controls. Consequently, the current security control baselines for NTIA's systems are not commensurate with the impact to NTIA's mission if the information contained in these systems became unavailable, exposed, or altered. Therefore, the current security controls do not meet the Department's security requirements to adequately protect its systems.

² Federal Information Processing Standard 199 provides security categorization guidance for non-national security systems. National Institute of Standards and Technology, February 2004. *Standards for Security Categorization of Federal Information and Information Systems*, FIPS 199. Gaithersburg, MD: NIST.

³ The National Institute of Standards and Technology outlined a six-step process to manage risks within an information system; security categorization is the first step. National Institute of Standards and Technology, February 2010. *Guide for Applying the Risk Management Framework to Federal Information Systems*, NIST SP 800-37. Gaithersburg, MD: NIST.

II. An Accurate Inventory of All Hardware and Software Components Is Essential for Ensuring Adequate System Security

NTIA did not properly identify all components of its systems and, therefore, has not identified the assets that need protection, nor can it provide assurances that security measures are properly implemented. Without an accurate, regularly maintained inventory of hardware and software components, the overall system and its information face increased risk of a successful attack through the exploitation of unmaintained and unauthorized components.

Hardware and Operating Systems

Our assessment of NTIA's network identified 44 servers that were not listed in NTIA's official inventory. This is almost double the number of officially reported servers. Our assessment also found two operating systems not listed in NTIA's official inventory. Because these servers and operating systems were not properly identified, the risks posed to NTIA's systems were neither appropriately conveyed to management nor appropriately managed. The following are some specific risks:

- A server running Microsoft Windows 2000 operating system. This product has not been supported by Microsoft since July 2010, and thus, critical security vulnerabilities have not been remediated, increasing the risk of compromise.
- Five servers owned and operated by the Commerce Office of Security on NTIA networks. Since there was a lack of formal agreement or assurance of implemented security controls on these servers, they pose additional risks to NTIA's systems. Similarly, NTIA's lack of security controls poses risks to the Office of Security's servers.
- Two operating systems (Windows 7 and VMware⁴) not listed in NTIA's inventory. These operating systems have unique requirements, which—if not addressed—can create significant vulnerabilities in NTIA's systems. For example, the addition of a virtual environment with VMware servers to support multiple operating systems and functions requires careful consideration. Operation of a virtual environment requires that both the host (VMware) and the guest (such as Windows or Linux) have implemented security controls. Identifying all operating systems is critical to determining key risk factors (specific risks posed by each new device or operating system).

⁴ VMware is a software product that provides virtualization. Today's computer hardware was generally designed to run a single operating system and a single application, leaving most machines vastly underutilized. Virtualization allows multiple virtual machines to run on a single physical machine, with each virtual machine sharing the resources of that one physical computer. Different virtual machines can run different operating systems and multiple applications on the same physical computer.

Unauthorized Software

We also found frequent instances of software, including extremely outdated and unsupported software such as Web browsers and music software, which was not identified in NTIA's baseline (i.e., the software that is authorized to be on the system). This indicates a lack of both definition and control over what software is installed within the system. Incomplete or inaccurate software baselines can introduce unnecessary vulnerabilities into a system.

Furthermore, we found unauthorized data files, related to movies and games, typically associated with peer-to-peer (P2P) file sharing technology, indicating that P2P software had previously been installed on some components. The Department prohibits the use of P2P technology unless it supports an official business requirement. Allowing system users to install and use this type of software increases the risk of introducing malware and can lead to violation of copyright laws.

Critical security requirements cannot be properly established until system hardware and software components are accurately identified. Further, a lack of controls to detect and remove unauthorized or outdated software can lead to malware being introduced into NTIA systems.

III. Deficiencies in NTIA's Plan of Action and Milestones Process Undermine Effective Remediation of Security Weaknesses

NTIA lacks an effective process to correct IT security weaknesses. The established and required mechanism to accomplish vulnerability remediation is the plan of action and milestones (POA&M) process. POA&Ms provide valuable oversight and communicate risk to management, the Department, the Office of Management and Budget, and system staff by conveying the status and number of IT security weaknesses that exist in a system. Management also uses POA&Ms when deciding whether to grant systems authorization to operate.

We found that NTIA was not using POA&Ms to document all known IT security weaknesses in five of its systems. For example, our assessments found that significant vulnerabilities, previously identified by an independent assessment of NTIA's networks in 2009, still exist but have not been documented in POA&Ms.

Conversely, when NTIA had created POA&Ms, they were not used to effectively track or remediate weaknesses. For example, we found POA&Ms were inappropriately closed or canceled because corrective action plans were too vague to implement or risk was inappropriately accepted without remediation. Many of the POA&Ms lacked critical elements such as milestones, due dates, or deadlines. When deadlines were established, they were not met. Half of all security weaknesses documented in POA&Ms remain unremediated and are classified as delayed.

Furthermore, NTIA management is not receiving information needed to determine the risk associated with unimplemented controls. NTIA has not followed the process required by Department policy to inform senior management about the status of security controls that cannot be fully implemented. The policy requires system owners to use POA&Ms to track and manage progress toward full implementation of required security controls. Our assessments found that when required security controls that have not been fully implemented are identified, POA&Ms are not created; rather, the associated risks have been accepted by the system owner. However, the authorizing official—not the system owner—is responsible for determining the acceptability of risk associated with unimplemented controls.

An effective process to remediate weaknesses is critical to an IT security program. NTIA management should establish this process immediately to ensure that corrective actions are appropriately planned and tracked.

IV. Inadequate IT Security Workforce Management and Lack of IT Security Policies Adversely Affect NTIA's IT Security Program

The major contributing factors to NTIA's serious IT security program deficiencies are weaknesses in the management of its IT security staff and the lack of program-level policies and procedures.

IT Security Workforce Management

NTIA has not taken the necessary steps to ensure that personnel with IT security responsibilities have appropriate training or certifications. At the time of our review, most of NTIA's IT security staff did not have the requisite knowledge or appropriate qualifications to implement and maintain the security measures necessary to protect the information stored and transmitted on a system. We found that 8 of 10 NTIA personnel with IT security responsibilities have not completed IT security training in the past 2 years and 9 of 10 do not have appropriate certifications (see table I for details).

According to Department policy issued in September 2010,⁵ personnel filling key IT security positions are required to obtain professional certifications or attend training annually based on their roles (see table I for details). If these staff members do not meet these requirements, NTIA must create a POA&M, identifying the risk to the organization posed by the staff members' lack of qualifications. At this time, NTIA has not identified the risks posed by these deficiencies, nor has it appropriately addressed them in POA&Ms.

Additionally, NTIA is not appropriately holding key IT security staff responsible for performing duties related to their positions. Department policy⁶ requires that performance

⁵ Commerce Interim Technical Requirements, September 2010, *Information System Security Training for Significant Roles Version 5.0*, CITR-006, Washington, D.C.: U.S. Department of Commerce, Office of the Chief Information Officer.

⁶ Memorandum from Deborah A. Jefferson, Deputy Chief Human Capital Officer and Director for Human Resources Management, and Suzanne Hilding, Chief Information Officer to Secretarial Officers and Heads of Operating Units,

plans for individuals in IT security roles include Department-specified responsibilities. For example, an information system owner is responsible for implementing and monitoring system security controls, and an information system security officer is responsible for creating and maintaining authorization documentation. For the past 2 fiscal years (FY 10 and FY 11), performance plans for 16 out of 17 IT personnel did not contain the required responsibilities. Furthermore, a review of FY 12 performance plans found that requirements for designation of responsibility are still unmet.

Table 1. Findings for NTIA IT Security Workforce Management and Policies

Key Position	Requirement	NTIA Compliance	Risk/Impact
Training			
Authorizing official	Minimum of 1 hour of role-specific IT security training	2 of 2 personnel did not meet this requirement for the current fiscal year. Nor had they received role-based training for the past 2 fiscal years.	People are the foundation of an effective IT security program and training is an important mechanism to ensure that they have the requisite knowledge, skills, and abilities.
Information system owner	Minimum of 2 hours of role-specific IT security training	6 of 8 personnel did not meet this requirement for the current fiscal year. Nor had they received role-based training for the past 2 fiscal years.	
Certification			
IT security officer, information system security officer, certification agent, and incident response responder	Approved security-related professional certification	9 of 10 personnel do not have an appropriate IT security certification.	Industry certifications provide greater assurance that staff has obtained a base set of IT security knowledge or skills.

Source: OIG Analysis and Department Policy

Note: During our audit fieldwork, the individual acting as NTIA's chief information officer (CIO) was not required to have CIO-related training; therefore, the total number of staff with training deficiencies does not include the CIO position.

December 7, 2009: *Information System Security Critical Elements (Stand-alone Elements or Collateral Duties)*; and memorandum from Deborah A. Jefferson, Deputy Chief Human Capital Officer and Director for Human Resources Management, and Suzanne Hilding, Chief Information Officer to Secretarial Officers and Heads of Operating Units, February 24, 2010: *Executive Critical Elements for Information System Security Roles*.

Program-Level Policies and Procedures

NTIA has not developed any bureau-level IT security policies or procedures for implementing Department and federal information security standards. While general IT security requirements are outlined in Department policy and in NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*,⁷ each bureau must evaluate these security requirements and develop policies and, more important, specific procedures to ensure that security requirements are defined, properly coordinated, and consistently implemented. The current practice at NTIA (because nothing has been defined at the program level) is to allow each system owner to independently interpret Department policy and NIST guidance. This uncoordinated approach, combined with a lack of appropriate training for its IT security staff, has contributed heavily to the inconsistent and inadequate security practices in NTIA's IT security program. The creation of program policies and procedures would ensure that organizational strategies, guidelines, and security roles are defined and communicated, providing greater assurance of an effective implementation of security measures necessary for the protection of NTIA's systems.

V. Significant Deficiencies in Key Security Areas Increase NTIA's Exposure to Cyber Attacks

NTIA has not sufficiently implemented security controls related to any of the areas we evaluated: account management, secure configurations, least functionality, vulnerability scanning and patch management, and auditing and monitoring.

Account Management

NTIA's Active Directory implementation is used to control user access to system resources and information. Although NTIA had made updates to accounts in its Active Directory implementation just before our review, we identified several issues relating to inadequate account management practices. Specifically, our assessment revealed active accounts for two users, who NTIA indicated were no longer working for NTIA. However, our assessment revealed that one of the accounts was for an individual who had accepted a position at NTIA but never started and that NTIA had no record of the other individual. This indicates a lack of coordination between human resources and information assurance personnel responsible for establishing and maintaining user access to NTIA's systems. The existence of an account for a user unknown to NTIA raises the concern that user accounts could be created for nefarious purposes yet go undetected. NTIA does not have any documented account management policies or procedures and thus lacks a process to help ensure that only legitimate users are provided access to information system resources. NTIA disabled these two accounts only after we informed management that they were still active.

⁷ National Institute for Standards and Technology, August 2009. *Recommended Security Controls for Federal Information Systems and Organizations*, SP 800-53. Gaithersburg, MD: NIST.

We also found 31 accounts, including 6 administrator accounts, with passwords that were not set to expire and thus never needed to be changed—a violation of Department policy, which requires that passwords be changed at least once every 60 days. Furthermore, we found that 114 (out of a total of 821) accounts that had not been accessed within 90 days of our assessment had not been disabled; 2 of these accounts had not been accessed since January 2010. Department policy requires disabling accounts after 30 days of inactivity.

Secure Configurations

NTIA has not defined or implemented required secure configurations for any IT products (i.e., operating systems and application software such as databases and Web applications). The definition and implementation of secure IT configurations are fundamental controls needed to secure an information system.

Least Functionality

NTIA has not performed the required process of limiting system and application functionality to ensure that only necessary services are enabled. The lack of definition and control over what software and services are authorized to operate on NTIA's systems leaves them open to additional risk by offering attackers opportunities for access to system components through open ports (doors through which an attacker can enter) and unauthorized software and services (such as websites, databases), having specific vulnerabilities.

We found 156 unique open ports on NTIA's workstations, and each port was identified on many different workstations. Specifically, we identified ports (1) running unauthorized Web servers that were operating websites, (2) commonly used by malicious software, and (3) running suspicious software⁸ (see table 2 for details).

⁸ Suspicious software is (1) unauthorized, (2) malicious, or (3) not defined as required to support legitimate functions and services within the system.

Table 2. Unique Open Ports Operating on NTIA's Workstations

Port Type	Risk	Impact	Number of Unique Open Ports
Web	Website vulnerabilities, additional avenue of external attack, operation of unauthorized websites	Additional risk of system compromise and information exposure	7
Malicious software	Operation of unauthorized software resulting in infected system components	Data exfiltration, further compromise of system components	19
Suspicious software	Operation of unauthorized software can introduce additional vulnerabilities	Provides avenues of access to a system and critical information	130
Total			156

Source: OIG Analysis

Additionally, NTIA has not developed policy or practices nor has it established a minimal operational baseline of ports and services for each IT system component (for example, servers, workstations, or applications) to implement least functionality. Until NTIA implements controls associated with least functionality, its information and systems will remain exposed to undue risk.

Vulnerability Scanning and Patch Management

NTIA's vulnerability scanning and patch management are not effectively identifying and remediating security weaknesses. Although NTIA scanned some of its systems, the scans were not performed with the required frequency. Furthermore, our review of one year's worth of scanning results found more than 30,000 vulnerabilities that went unremediated with no POA&Ms created to track them. In addition, our assessment of NTIA's databases identified significant and easily exploitable vulnerabilities that could lead to SQL injection⁹ or privilege escalation attacks.¹⁰

Auditing and Monitoring

NTIA has not implemented an auditing and monitoring program, and its current plans do not meet Department requirements or provide assurances for the effective monitoring of risks to its information. Auditing and monitoring are critical to the security of an organization's systems and information, because by auditing and monitoring real-time

⁹ SQL injection is a technique often used to attack databases through a website.

¹⁰ A privilege escalation attack is a type of network intrusion that takes advantage of programming errors or design flaws to grant the attacker elevated access to the network and its associated data and applications.

activity and access to a system, an organization can better identify attacks on and compromises of its systems and information. Department policy and NIST standards require operating units to actively monitor their systems and information for suspicious activity, investigate such activity, and report their findings to officials.

NTIA plans to have audit logs available for analysis, but does not plan on actively monitoring its systems for malicious activity; it will rely on the Herbert Clark Hoover Building's Security Operations Center to provide notification of security events. However, the Security Operations Center only monitors external security events and does not monitor activity on NTIA's internal networks.

Conclusion

Although the IT security controls we assessed have been required for all Department systems since 2006, NTIA has not taken fundamental steps to implement these controls. Therefore, greater attention from management is needed to ensure that NTIA's systems and information are adequately secured. NTIA staff has been briefed on our technical assessment results and is taking action to correct the deficiencies identified.

Recommendations

To make NTIA's information security program and practices more effective, the Assistant Secretary for Communications and Information should ensure the following:

1. Revise the authorization status of NTIA's systems to interim authorization to operate until the following activities have been completed:
 - a. system owners and appropriate NTIA officials collaborate to identify and categorize all information types that are processed, stored, or transmitted by each system and categorize each system accordingly,
 - b. system owners develop and maintain an accurate hardware and software inventory for their systems,
 - c. NTIA implements and assesses appropriate IT security controls according to Department policy and NIST SP 800-53, and
 - d. NTIA follows the POA&M process required by the Department's IT security policy.
2. System owners, IT security officers, authorizing officials, and other staff with critical IT security roles are appropriately trained, earn certifications as required by Department policy, and have the required metrics incorporated into their performance plans.
3. NTIA's chief information officer and IT security officer develop and maintain NTIA security policies, procedures, standards, and guidance consistent with departmental and federal requirements.

Summary of Agency Response and OIG Comments

In response to our draft report, the Assistant Secretary for Communications and Information stated that NTIA concurred with our findings and is taking appropriate action to address them. The response also summarized the steps NTIA has implemented and will take to address the recommendations.

We met with NTIA officials to verify concurrence with our recommendations and to clarify the following statement in NTIA's response: "However, NTIA cannot validate the OIG assertion that five NTIA systems have been miscategorized." According to NTIA officials, the statement is meant to convey agreement that NTIA had performed inadequate categorization analysis on the systems and, at the time NTIA issued its response to our draft report, that NTIA had not completed the categorization process, which includes identifying all the information types that exist within its systems. NTIA did concur with our recommendations and agreed that OIG's analysis was correct.

Appendix A: Objective, Scope, and Methodology

Our objective was to assess the effectiveness of NTIA's IT security program by determining whether key security measures adequately protect its systems and its information. To do so, we

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

We reviewed NTIA's compliance with the following applicable provisions of law, regulations, and mandatory guidance:

- 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, 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
 - 800-18, Guide for Developing Security Plans for Information Technology Systems
 - 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems
 - 800-53, Recommended Security Controls for Federal Information Systems and Organizations

- 800-53A, Guide for Assessing the Security Controls in Federal Information Systems
- 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories, Volumes I and II
- 800-70, National Checklist Program for IT Products—Guidelines for Checklist Users and Developers
- 800-115, Technical Guide to Information Security Testing and Assessment

We conducted our fieldwork from February to May 2012. 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.

Appendix B: Agency Response



UNITED STATES DEPARTMENT OF COMMERCE
The Assistant Secretary for Communications
and Information
Washington, D.C. 20230

AUG 15 2012

SUBJECT: NTIA Response to the Office of Inspector General's Draft Report, *Significant IT Security Program Improvements Are Needed to Adequately Secure NTIA's Systems*

FROM: Lawrence E. Strickling 

TO: Mr. Allen Crawley
Assistant Inspector General
Office of the Inspector General

Thank you for the opportunity to comment on the Office of Inspector General's Draft Report, *Significant IT Security Program Improvements Are Needed to Adequately Secure NTIA's Systems* (the Report). Your comprehensive review of the NTIA IT security program documents a situation with our IT security program in response to which we are already taking appropriate action to remedy. A summary of our response to your specific findings is attached.

Since your review of NTIA's IT security program in March, NTIA strengthened its IT management team by hiring a new Chief Information Officer in April and Deputy Chief Information Officer in July. I have tasked NTIA's new IT leadership with improving NTIA's IT operations, specifically focusing on IT security management, asset control, remediation improvement, workforce management, and security controls oversight. NTIA already demonstrated improvement in IT security during a Department of Defense (DOD) inspection in May, 2012. The DOD inspection of security baselines and vulnerability management of selected NTIA systems resulted in a rating of "Excellent".

However, as your Report notes, NTIA still must overcome a number of IT security challenges. We have made significant progress in the areas addressed in the Report, including: establishing an Inter-Agency Agreement with the DOD (SPAWAR) to provide resources to review security categorizations and complete Authorization and Accreditations of systems; completing a total IT asset inventory; clarifying and improving accountability for NTIA security roles and responsibilities; aligning security management operations with Department guidance; establishing 17 security policies (with plans for an additional four); and remediating many identified deficiencies in IT security controls.

We recognize the important role of the OIG in promoting improvements in operating unit practices and conformance to applicable departmental and federal requirements. As outlined in the Attachment, we have taken immediate steps to address each recommendation presented in your report.

NTIA is committed to becoming an exemplary agency for IT management. I look forward to working with you as NTIA continues to address the recommendations in the Report and

improves the protections required to secure NTIA's systems. If you have any questions regarding this response, please contact Milton Brown, NTIA's Audit Liaison, at (202) 482-1853.

cc: Simon Szykman, Chief Information Officer
Griff Drew, Chief Information Officer, NTIA
Tim Hurr, Acting Director, Office of Cyber Security
Milton Brown, Audit Liaison, NTIA
Susan Schultz Searcy, Audit Liaison, Office of the Chief Information Officer

Attachment

Response to Findings Regarding Security Categorization

The most basic and important step of protecting NTIA's IT systems is to properly perform an initial Authorization and Assessment (A&A) and to maintain that assessment during the lifecycle of the system. The NTIA A&A process, based on the DOC guidance, requires the system owner to perform the Federal Information Processing Standard (FIPS) 199 security categorization process.

NTIA concurs with the finding that NTIA information technology systems have inadequate categorization analysis. Through efforts performed after the OIG assessment and during the transition to the new Chief Information Officer (CIO), NTIA confirmed that the FIPS 199 process review was not consistently performed. However, NTIA cannot validate the OIG assertion that five NTIA systems have been miscategorized.

NTIA has confirmed that the FIPS 199 process was performed by the System Owners with support from technical staff, but without input from critical end users. NTIA agrees with the OIG approach of performing end user interviews, discussing with the system owners, and evaluating the system categorizations. The NTIA CIO is working with System Owners to revisit system categorization, ensuring the inclusion of critical end users, and is actively seeking outside expert assistance to lead the discussion and analysis in performing a re-validation of FIPS 199 processes for all NTIA systems. NTIA has already recategorized one of the systems referenced by the OIG.

At least one of the systems, the NTIA General Support System, referenced as miscategorized in the Report is not completely controlled by NTIA. If, during the recategorization process, the system's categorization level changes, NTIA will have to work with the Department OCIO to determine how to implement the appropriate controls or how to isolate the information from the larger IT system.

Response to Findings Regarding Accurate Inventory

Hardware and Operating Systems

NTIA concurs with OIG's assessment that we did not properly identify all components of our systems. Since the OIG audit, NTIA has performed a complete physical inventory of all IT assets, and has reflected all inventory updates in the Department's Sunflower system. In addition, we decommissioned several older systems, including the Windows 2000 server, from operation. In fact, since the OIG inspection, NTIA has disposed of over 18 physical server assets and updated the appropriate hardware and software inventories to reflect these changes.

NTIA has completed an updated agreement with the Department's Office of Security for the hosting of five servers at NTIA's continuity of operations site and has accurately reflected those systems in the NTIA inventory.

NTIA addressed the issues with Windows 7 and VMWare by adding them to the list of approved and supported operating systems. In addition, we are implementing automated methods of software discovery and a Configuration Management Data Base (CMDB) that will regularly scan NTIA systems and compare software changes against the documented and locked baseline. We anticipate the CMDB will be operational in second quarter FY 2013.

Unauthorized Software

NTIA concurs with OIG's finding of unauthorized, unapproved software installed on NTIA computers. We implemented regular review of software scans (weekly) that provide detailed information concerning software installed on NTIA systems. Following the established change management process, we create help desk requests for software deletion or update based on the analysis of the scan findings. As mentioned above, the installation and operation of a CMDB will regularly scan the NTIA systems and compare software changes against the documented and locked baseline.

As part of our Windows 7 installation – which is currently underway – NTIA is zero-baselining all installed software. End users will not have permission to install software on computers. Any deviations from the approved baseline configuration require review and approval from the NTIA Information Assurance team and the CIO. After approval, the software will be added to the NTIA Software Whitelist and subsequently installed on the system.

In addition, NTIA is currently documenting appropriate use policies that will ensure users are aware of the software approval process and DOC and NTIA prohibitions.

Response to Findings Regarding Deficiencies in NTIA's Plan of Action and Milestones (POA&M) Process

NTIA agrees with the OIG's finding that, at the time of the OIG assessment, NTIA lacked an effective process to correct IT security weaknesses. After filling the CIO vacancy, NTIA began documenting and following a structured process for identification, validation, and remediation of vulnerabilities for all NTIA systems. We have made significant improvements in the POA&M creation and resolution process. As part of this process, NTIA scans unclassified systems weekly and distributes the results to the Network Engineering and Operations Branch (NEO) for analysis and remediation. NEO develops POA&Ms for any deficiencies that cannot be remediated within 90 days. After review with the CIO for feasibility and timeliness, NTIA enters that information into the Department's Cyber Security Assessment and Management (CSAM) system. As of the third quarter FY 2012, NTIA has begun reporting to the Department on the status of POA&M milestones. In the third quarter, 67% of POA&Ms were closed on time.

NTIA is still maturing with the implementation of and requirements for updating CSAM. However, we can now provide detailed information about all POA&Ms impacting NTIA systems, including a POA&M specifically targeted at remediation of all items identified as part of this audit.

Response to Findings Regarding IT Security Workforce Management and IT Security Policies

NTIA agrees with the OIG's statement that the major contributing factors to NTIA's serious IT security program deficiencies are weaknesses in the management of its IT security staff and the lack of program-level policies and procedures. NTIA also would add that the lack of defined security roles and responsibilities has exacerbated the issue associated with IT security staff management.

IT Security Workforce Management

Under the advice of the NTIA CIO, NTIA has updated and published new IT Security Roles and Responsibilities. These roles ensure that the CIO is the Authorizing Official for all NTIA systems, unless properly delegated. In addition, we have consolidated all of the IT Security Officer (ITSO) and Information System Security Officer (ISSO) roles within the NTIA Information Assurance Program Branch, significantly reducing the number of NTIA staff who require specialized training and certifications.

Based on these new roles, NTIA has established a plan for the completion of all associated training and required certifications. We have documented this plan in a POA&M and input it to CSAM as required by Department policy.

Additionally, the staff with significant IT security roles will have information system security critical elements and metrics incorporated in their FY 2013 performance plans. Performance plans for Authorizing Officials and Information System Owners will contain a stand-alone security element in FY 2013 as required by the CIO's June 29, 2012 memorandum.

Program-Level Policies and Procedures

NTIA agrees that each bureau must develop and evaluate security requirements and implement associated policies, and more importantly, specific procedures, to ensure that security requirements are defined, properly coordinated, and consistently implemented. NTIA's CIO and IT security officer, supported by NTIA and contractor staff, have identified 21 IT security policies, with associated procedures and guidance, that require development. NTIA has developed draft copies of 17 policies that are currently under review and is working on the additional four policies. Once completed and coordinated, these policies will be posted on the NTIA Intranet to provide all users awareness and access to the policy guidance. NTIA will also disseminate all procedures to technology staff to ensure that security policies are consistently implemented.

Response to Findings Regarding Deficiencies in Key Security Areas

NTIA agrees with the OIG's finding that, at the time of the assessment, NTIA had not sufficiently implemented security controls related to all evaluation areas. As noted in the Report, NTIA has taken action to correct the IT security control deficiencies identified by OIG, including:

- Active accounts existing for user names that don't correspond to employees listed
- Expired accounts – active accounts with last login > 90 days ago
- Open ports
- Passwords not required
- Passwords not expiring on active (i.e., not disabled) accounts
- Possible unauthorized software instances

Account Management

NTIA has drafted an Access Control Policy to address proper account management policy. In addition, we have documented the proper account management procedures that correspond to the draft policy.

Secure Configurations

NTIA has drafted a Configuration Management Policy to address the establishment and management of secure baseline configurations. Once the policy is finalized, NTIA will document the baseline security configurations, document the appropriate settings in the CMDB, and then use automated scanning and validation tools to identify any changes to the approved security baseline.

Least Functionality

NTIA agrees that we have not performed the required process of limiting system access and application functionality to ensure only necessary services are enabled. We believe this is a core component in the establishment of the secure baseline configurations and will address this finding during the development of these baselines.

NTIA has drafted an Access Control policy to address the requirement for Least Functionality and that Least Functionality analysis must be included in the development of each IT system prior to deployment. To support the implementation of this policy, NTIA is actively researching automated tools to assist with the identification of potentially risky privileges on NTIA systems with a plan to implement this tool in the quarter of FY 2013.

Vulnerability Scanning and Patch Management

NTIA has made significant strides in improving our vulnerability scanning and patch management processes. NTIA has drafted a Vulnerability Management Policy to document the

requirement and timeline for identification and application of all security vulnerabilities and other critical system patches.

NTIA has reduced the total number of vulnerabilities, which the OIG reported as greater than 30,000, to less than 2,000. We accomplished this through the application of weekly scanning and patching, and a POA&M identification process that has produced a commitment to vulnerability management at NTIA. In addition, the NTIA CIO held a technology all hands and personally briefed all staff with technology roles on the policy, process, and expectations as related to vulnerability management.

To support the implementation of this policy, NTIA is actively exploring automated technology that will test application and database weaknesses to identify potential vulnerabilities such as SQL injection and privilege escalation attacks. Once identified, these weaknesses will either be placed on a POA&M for action or the subject system will be scheduled for replacement.

Auditing and Monitoring

NTIA agrees that we do not have an active plan to implement an auditing and monitoring program. NTIA has drafted an Audit and Accountability Policy to address the requirement for an auditing and monitoring program. Once this policy is approved, NTIA will develop a strategy for implementing the program, including the possibility of working with the Office of Networking and Telecommunications Operations (ONTO) for a solution that supports all of HCHB.

Conclusion

NTIA concurs that all OIG findings were valid at the time of the assessment. We believe that with the staffing of two critical positions and increased focus on IT security management, NTIA has made significant progress in improving our technical capabilities and developing the required policies and procedures to provide a high-performing, secure technical environment for all systems. Through the implementation of planned improvements, NTIA hopes to continue to make progress in addressing the information security concerns highlighted in the Report and strengthening the management of NTIA's IT program.

011200000142