Audit of NARA's Intrusion Detection and Prevention Systems and Incident Response

OIG Audit Report No. 13-12

September 10, 2013

Table of Contents

Executive Summary

Intrusion detection and prevention systems (IDPSs) detect, monitor, analyze, and prevent possible malicious activity occurring in computer systems or a network. Incident response is a process to analyze and resolve an incident to minimize adverse effects. The National Archives and Records Administration (NARA) Office of Inspector General (OIG) audited NARA's IDPSs and computer security incident response process to determine whether: (1) NARA's IDPSs had been properly implemented and are operating effectively; (2) appropriate logical and physical security, and environmental protection controls are in place, and; (3) NARA's computer security incident response process is effective and efficient, including whether incident response staff are adequately trained.

In general, it appears NARA's IDPSs are operating effectively, and incidents are appropriately handled. However, opportunities for improvement exist in areas including:

(a) logical security and configuration of the host intrusion prevention system;
(b) contract management and monitoring;
(c) incident response and incident reporting to United States Computer Emergency Readiness Team (US-CERT); and
(d) physical security controls on the host intrusion prevention servers.

First, an excessive number of privileged user accounts existed on NARA's centralized host-based intrusion prevention system (HIPS)[1] and anti-virus management application, and the password policy was not systematically enforced for users at the application level. This left the application, rule sets, and data within the application vulnerable to inappropriate use, manipulation, or deletion. Also, not all machines connected to NARANet report to the centralized HIPS and anti-virus management application, making it difficult to assess and monitor the security status of the machines not reporting to the application on a real-time basis.

Further, NARA had not effectively managed and monitored its contract with the Trusted Internet Connections (TIC) provider. This resulted in unmet Acceptable Quality Levels (AQLs) for a number of services; unclaimed service credits; and a disconnect among the contractor, Designated Agency Representatives (DARs), and NARA's IT staff in transferring and exchanging information pertinent to the security of NARA's IT environment.

[1] A host-based intrusion prevention system is a type of IDPS that monitors characteristics of a single host and the events occurring within that host for suspicious activity (NIST SP 800-94, February 2007; p.9).

Additionally, although network attacks evolve over time and are becoming more sophisticated, there is no process at NARA to ensure internal or external training is given to the Computer Incident Response Team (CIRT) so they remain up to date. Also, the incident handling process was not always monitored and supervised properly, causing delayed resolution and reporting of incidents. Approximately 75% of sampled computer security incidents reportable to US-CERT were not reported on time.

As part of this audit, we also reviewed non-electronic, paper-based disclosure of personally identifiable information (PII) incidents. OMB Memorandum M-06-19 specifies US-CERT reporting should include all personally identifiable information (PII) incidents whether in electronic or physical form. Our review found a weakness related to NARA's handling of paper-based PII disclosure events, which is addressed in a separate report (OIG Report No. 13-15).

Finally, opportunities to improve physical security controls exist at NARA's computer room at Archives II. Specifically: (1) the list of the individuals who have access to the computer room had not been reviewed on a periodic basis; (2) visitor logs were incomplete and had not been reviewed on a periodic basis; and (3) cables for certain servers were poorly organized without the use of any cable management tools such as labels and ties.

This report contains 18 recommendations which, upon implementation, will enhance NARA's ability to secure its IDPS devices and respond to computer security incidents effectively.

Background

Various organizations at NARA contribute to the security of its computing environment and electronic data. IT Security (IT) is responsible for the overall security of NARA's IT environment. IT Operations (IM) manages NARA's HIPS and anti-virus applications, configuration of the network-based intrusion detection system (NIDS)[2], and the Networx Universal program[3]. Both IT and IM are sub-organizations under the Office of Information Services (I). The CIRT, comprised of NARA's IT Security and IT Operations staff, performs computer security incident response and reports incidents to US-CERT and works with other investigative agencies when necessary. In addition, Business Support Services (B) oversees physical security and environmental protection controls for NARA's computing equipment stored in each NARA location, including the IDPS management and database servers.

NARA also uses the intrusion detection/prevention and incident response services provided by the TIC contractor in accordance with the Managed Trusted Internet Protocol Services (MTIPS) under the United States General Service Administration (GSA)'s Networx Universal program. The TIC contractor operates the NIDS and Security Operations Center (SOC). NARA's CIRT and the contractor's SOC interact with one another in detecting, analyzing, and resolving computer security incidents. The TIC contractor also provides a co-location service for NARA-owned firewalls and hosts the EINSTEIN[4] enclave that includes the IDPS appliances maintained and operated by United States Computer Emergency Readiness Team (US-CERT).

NARA is a subscribing agency of GSA's Networx Universal program, and selected the TIC contractor in October 2010. The contractor completed installation of the TIC at NARA in July 2011. According to GSA's Networx Service Level Agreement (SLA) Management Guide, version 2.0, issued on April 30, 2009, it is the subscribing agency's role to: (1) review the Monthly Compliance Reports submitted by the service provider; (2) identify discrepancies between the contract-required performance target and the actual performance; and (3) apply for credit from the service provider for a failure to meet a performance objective.

[2] A network-based intrusion detection system monitors network traffic for particular network segments and analyzes the network activity to identify suspicious activity (NIST SP 800-94, February 2007; p.9).
[3] Networx offers managed security services through the MTIPS program, which complies with the Trust Internet Connections (TIC) initiative (http://www.dhs.gov/managed-trusted-internet-protocol-services.
[4] The Einstein program provides an automated process for collecting, correlating, analyzing, and sharing computer security information across the Federal Government to improve our nation's situational awareness (http://www.us-cert.gov/government-users/tools-and-programs).

US-CERT requires Federal agencies to report computer incidents in accordance with specified timeframes that vary depending on the category and severity of the incident. As of December 5, 2012, NARA had a total of 298 closed incidents in its incident management system that were reportable or potentially reportable to US-CERT and submitted between July 28, 2011, and October 11, 2012. Distribution of the incidents by incident category and location of the ticket origination is shown on **Table 1** below.

Table 1: Distribution of Incidents by Category and Ticket Origination

Site\Incident Category	Disclosure of PII	Malicious Logic	Improper Usage	Attempted Access	Investigation	Grand Total
Archives I		10				10
Archives II	198[5]	56	2	4	5	265
Carter Library		1				1
Dayton		1				1
Eisenhower Library		1				1
Hoover Library		1				1
Johnson Library		1				1
Philadelphia		2				2
Riverside		1				1
Spanish Lake		12				12
St Louis		1				1
Suitland		1				1
Valmeyer		1				1
Grand Total	**198**	**89**	**2**	**4**	**5**	**298**

Previous audit engagements between fiscal years (FYs) 2005 and 2012 identified weaknesses in NARA's IDPSs and incident response process. These weaknesses included: (a) lack of host-based sensors to detect intrusions (OIG Audit Report No. 05-09, dated April 1, 2005); (b) inconsistent incident response approaches among the incident response team (Mandiant's Incident Response Program Enhancement Gap Analysis, dated May 17, 2010); (c) partially deployed centralized HIPS and anti-virus management system (Mandiant's Incident Response Program Enhancement Gap Analysis, dated May 17, 2010); (d) lack of a process to manage and monitor the Service Level Agreements (SLAs) associated with its Networx contract (OIG Audit Report No. 11-17, dated September 30, 2011); and (e) open, unsecured network topology (IMRI's Network Discovery and Assessment Report, dated August 27, 2012).

[5] OMB Memorandum M-06-19 specifies US-CERT reporting should include all PII incidents whether in electronic or physical form. Table 1 may include computer-based, electronic PII disclosures caused by loss or disclosure of encrypted or unencrypted PII data, and paper-based PII disclosures caused by mailing incorrect military/civilian records to the requesters. Archives II originates PII-related tickets for all offices.

Objectives, Scope, Methodology

The objective of this audit was to determine whether: (1) NARA's IDPSs had been properly implemented and are operating effectively; (2) logical and physical security and environmental protection controls are in place to appropriately safeguard NARA's IDPS devices and the data within them; and (3) NARA's computer security incident response process is effective and efficient, and the incident response staff are adequately trained. Additionally, we included a review of the controls in place at NARA's TIC provider over the IDPS and incident response process in our audit.

To accomplish our audit objective, we reviewed National Institute of Standards and Technology (NIST) Special Publications 800-53 "Recommended Security Controls for Federal Information Systems and Organizations," Revision 3[6], August 2009; 800-94 "Guide to Intrusion Detection and Prevention Systems (IDPS) (Draft) ," Revision 1, July 2012; and 800-61 "Computer Security Incident Handling Guide", Revision 2, August 2012. We also reviewed previous audit and review reports including OIG Report No. 05-09 Audit of NARA's Intrusion Detection System, dated April 1, 2005; OIG Report No. 10-07 Audit of NARA's Network Infrastructure, dated April 28, 2010; OIG Report No. 11-17 Audit of the Trusted Internet Connections Initiative at NARA, dated September 30, 2011; GAO's report on NARA's information security, dated November 2010; Mandiant's Incident Response Program Enhancement Gap Analysis, dated May 17, 2010; and OIG Report No. 12-11 Information Management Resources, Inc. (IMRI's) Network Assessment Report, dated August 27, 2012.

We judgmentally selected a sample of 80 security incidents that were reportable or potentially reportable to US-CERT, and were opened between October 2011 and October 2012. We reviewed the sampled incident reports and email communications from/to US-CERT and the contractor to determine whether appropriate actions were taken to resolve and report the incidents effectively and efficiently.

We interviewed representatives of the Office of Information Services (I) and NARA's main IT contract, the IT and Telecommunications Support Services **(**NITTSS**)** contract, and obtained and reviewed supporting documents as available and necessary. These supporting documents included, but were not limited to, policies and procedures, network diagrams, screenshots, physical and logical access lists, sample computer security incident reports, the Networx contract, Networx SLA Management Guide issued by GSA, the TIC contractor's Monthly Compliance Reports, and third-party evaluation reports for

[6] NIST SP 800-53, Revision 4, was issued in April 2013, which was after the fieldwork for this audit was substantially completed.

the TIC contractor issued by Department of Homeland Security and an independent public accounting firm. We visited two of the TIC contractor's data center facilities located in Sterling, VA, and had conference calls with individuals at the contractor's Network Operations Center (NOC) and Security Operations Center (SOC), located in Arlington, VA, and San Diego, CA, respectively. We also visited one of NARA's computer rooms at Archives II to assess the physical security of NARA's in-house host-based intrusion detection system servers.

Our audit work was performed at Archives II in College Park, MD, between October 2012 and June 2013. We conducted this performance 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 based on our audit objectives.

Audit Results

1. Logical Security of the Host-Based IDS (HIPS) Needs to be Strengthened

Overall, we found the centralized HIPS and anti-virus management system (the system) appeared to function effectively. It uses the "pull" method[7] to update the HIPS and anti-virus signatures on a daily basis, using a digital signature algorithm signature verification system for data integrity. When events occur which the system cannot automatically handle, it sends a notification email to NARA's IT security contractors with event details including the source Internet Protocol (IP) address, threat name, and detecting product name(s). The system can generate many types of queries and reports, such as a report including the signature update status of the servers and workstations. The management server and database server of the system reside on a Virtual Local Area Network (VLAN), and users log on to the system using a HTTPS connection to secure the communication.

However, a number of issues may prevent management from adequately securing the system, the machines managed through the system, and the machines not connected to the system. Specifically, we found there are too many super users, password parameters do not exist at the application level, the rule sets within the system had not been considered for customization, and only some of the machines connected to NARANet are configured to report to the system. These issues exist because management relies heavily upon the network-based intrusion detection system (NIDS) provided by the TIC contractor and had put little emphasis on adequately securing the centralized HIPS and anti-virus management system and maximizing the use of the system. As a result, these security issues present the risk of: (1) the users' accounts and the data within the system being compromised; (2) security events not being detected and prevented in a timely manner; and (3) being unable to assess the security status of the machines not reporting to the system on a continuous, real-time basis.

Too Many Super Users

NARA's Enterprise Architecture requires, in accordance with the Access Control (AC) family of the NIST Special Publication 800-53, that for data requiring moderate or high

[7] Pull is a style of network communication where the initial request for data originates from the client, and then is responded to by the server.

confidentiality, the NARA system owner shall employ the concept of least privilege. Least privilege only allows authorized access for users which are necessary to accomplish assigned tasks in accordance with NARA missions and business functions. System owners shall also limit authorization for super user[8] accounts on the information system to designated system administration personnel.

Within the centralized HIPS and anti-virus management system, we found that nine of the 10 users had been granted global administrator rights. According to the product guide for the system, the permissions exclusive to global administrators include: (a) creating, editing, and deleting source and fallback sites; (b) changing server settings; (c) adding and deleting user accounts; (d) adding, deleting, and assigning permission sets; and (e) importing events into the database and limiting events stored there. The NARANet Information System Security Officer (ISSO) stated the global administrator rights were required to run queries and reports. However, our review of the product guide found a regular user could be assigned to a permission set that allows the user to run queries and reports.

Granting global administrator access to an excessive number of users presents the risk of rights being abused by one or more users and undesirable changes made to user accounts, rule sets, and other configurations. Those changes may result in: (1) a valid user unable to log on to his/her account or unable to access certain functionalities necessary for their job responsibility; (2) an intrusive attack going undetected or unanalyzed; and (3) diminished productivity due to the need to reconfigure the system to its previous state.

Nonexistent Password Parameters

NARA's Enterprise Architecture requires, in accordance with the Identity and Authentication (IA) control family of the NIST Special Publication 800-53, that for all data, the information system shall enforce minimum password complexity of a case-sensitive, 8-character mix of upper case letters, lower case letters, numbers, and special characters, including at least one of each. It also requires that the information system enforce at least a four-character change when new passwords are created, encrypts passwords in storage and in transmission, enforces password minimum and maximum life time restrictions from one to 90 days, and prohibits reusing the previous five passwords for unclassified information systems or 10 passwords for classified information systems.

Although NARA's centralized HIPS and anti-virus management system requires a username and password to log in, it does not systematically enforce any password

[8] A super user, or a system administrator, is an account that has access to all files and can execute any type of command within the system. Global Administrator accounts within the centralized HIPS and anti-virus system are considered super users because they have read and write rights to all operations of the system.

parameters including length, complexity, and reuse restriction at the application level. We requested a read-only user account for the system and attempted to change the password to one as simple as a "0." The system accepted the password. Also, we were able to change the password back to the original password without any restriction for reuse. According to the NARANet ISSO, the capability to enforce password parameters does not exist within the system, which is a COTS (commercial off-the-shelf) limitation. However, our review of the product guide found there is an option to configure the system server to allow users to log on using Windows authentication, through which stronger password parameters could be enforced. According to the Chief Information Security Officer (CISO), the mitigation NARA had been depending on was a claim people who have accounts on the system are believed to be "trusted users," who could be expected to practice good password discipline.

We inquired with the NARANet Information System Security Officer (ISSO) whether passwords were encrypted within the system. According to NARA Directive 804.8, the ISSO has the responsibility to ensure the appropriate operational security posture is maintained for IT systems and programs. NARA's Enterprise Architecture requires passwords to be encrypted in storage and in transmission. The ISSO should be aware of the requirement, and ensure the systems they manage are appropriately configured to meet the security requirements. However, the NARANet ISSO was unable to answer whether the passwords were encrypted. Not enforcing strong password parameters and password encryption exposes the user accounts to the risk of being compromised, and critical data necessary to investigate intrusive attacks within the system being manipulated or deleted by an unintended user.

During this audit, we communicated the issue of unenforced password parameters to some of the key IT Security personnel, including the NARANet ISSO and CISO. According to the CISO, an option to implement more vigorous password policy is to have the user accounts authenticate to the Novell e-Directory. According to CISO, he had notified the NITTSS contractor to expect a request for a technical recommendation on this implementation.

Customization Needed on HIPS Rules

According to NIST Special Publication 800-94, most IDPSs require at least some tuning and customization, such as setting the prevention action to be performed for particular alerts, to improve their detection accuracy, usability, and effectiveness. NARA utilizes the vendor's default "Basic Protection" option for its HIPS. According to the evidence presented, the Basic Protection option prevents events whose signature severity level is "High" but ignores any events with signature severity level of "Medium", "Low", or "Information". There are other protection options available including "Enhanced

Protection" and "Maximum Protection" within the system. The Enhanced Protection prevents events with signature levels of High and Medium, and the Maximum Protection prevents events with signature levels of High, Medium, and Low. According to the NARANet ISSO, NARA decided to adapt the vendor's default protection option and did not consider implementing the other options. Selecting the option that only prevents the "High" events may not detect or prevent some of the actual intrusive attempts that could potentially have critical impact on the affected machine, the data within the machine, and the network to which it is connected.

Centralized Management System Not Fully Deployed

According to NIST Special Publication 800-94, organizations should consider using multiple types of IDPS technologies to achieve more comprehensive and accurate detection and prevention of malicious activity, with lower rates of false positives and false negatives. Also, for most environments, a combination of network-based and host-based IDPS technologies is needed for an effective IDPS solution. In Mandiant's Incident Response Program Enhancement Gap Analysis conducted in 2010, Mandiant recommended NARA deploy the HIPS application to all NARA Windows systems in all domains, and deploy the centralized HIPS and anti-virus management system to all NARA Windows systems (servers, workstations, and laptops) in all domains. We found the HIPS application is installed on the machines with Windows platforms that are connected to NARANet. According to the NARANet ISSO, the non-Windows-platform machines connected to NARANet have the antivirus software installed, but not the HIPS. We also found that not all of the systems connected to NARANet interact with the centralized HIPS and anti-virus management system to report events and receive signature updates.

NARA has a number of systems not reporting to the centralized HIPS and anti-virus management system, including [redacted] are the systems critical to achieving NARA's mission as the nation's record keeper, and the FIPS 199 Risk Impact Level of these systems for FY 2012 was "High." According to the Senior IT Security Specialist, these systems pass through the TIC contractor's network-based intrusion detection system (NIDS) and NARA's internal firewalls to pass and receive external traffic. However, these systems do not report to the centralized HIPS and anti-virus management system, making it difficult to continuously monitor the security status of the machines (e.g., whether an anti-virus program is installed and operating on the machine) or to centrally manage signature updates and event logs. Moreover, the FY 2012 FISMA evaluation revealed NARA had not developed and implemented fully integrated and responsive continuous monitoring and auditing capabilities allowing the organization to

manage risk more effectively and efficiently. With the lack of a fully integrated and responsive continuous monitoring process for security of NARA's information systems, NARA is under the risk of compromised systems not being promptly detected and resolved.

Recommendations

We recommend NARA's Chief Information Officer:

1. Evaluate the access requirements each user needs to perform their job responsibilities, limit the global administrator privilege to only those whose job responsibilities require the exclusive permissions, and establish permission groups allowing users to access limited reports or functionalities within the system.
2. Systematically enforce password parameters for system users at the application level consistent with NARA's Enterprise Architecture password requirements.
3. Consider re-evaluating the rule sets currently in use by the system for detection accuracy and customizing them to potentially reduce the number of intrusive attempts going undetected.
4. Consider conducting a cost-benefit analysis on deploying the system to all NARA unclassified systems connected to the network.

Management Response

Management concurred with the recommendations.

2. Contract Monitoring for MTIPS Needs Improvement

NARA is a subscribing agency of GSA's Networx Universal contract, through which NARA selected a provider for its Trusted Internet Connections (TIC) services. According to GSA's website, the Managed Trusted Internet Protocol Service (MTIPS) program provides managed security services compliant with Trusted Internet Connections initiatives. NARA's TIC contractor started providing services in July 2011. From January 2012 to December 2012, NARA paid a total of $3,236,853.26 (a monthly average of $269,737.77) for the entire contract.[9]

OIG Audit Report No. 11-17, Audit of the Trusted Internet Connection Initiatives at NARA, dated September 30, 2011, revealed that a process had not been developed to

[9] The services provided by the contractor include co-located hosting of NARA's MTIPS devices, configuration/rule change management, intrusion detection/prevention security event notification, and security incident reporting to NARA and US-CERT.

monitor the contractor's performance. We found the process for monitoring the contractor's performance is still yet to be fully developed. We also found there is a disconnect among the contractor, Designated Agency Representatives (DARs), and NARA's IT staff in regard to how some of the contractor's responsibilities are being, or should be, performed. This occurred because NARA relies heavily on GSA's monitoring and accreditation process, and had not developed a more vigorous contract monitoring and management process. As a result, we found the following, which are discussed in more detail in the next sections:

- The actual performance data for a MTIPS service was not included in the contractor's Monthly Compliance Reports for the entire period reviewed (January 2012 through December 2012);
- There were at least two instances within the period reviewed where the Acceptable Quality Levels (AQLs) were not met by the contractor, for which NARA could have requested credits; and
- NARA's key IT Security staff was not aware the intrusion prevention capability was not enabled within the IDPS device for NARA's network.

Contract Management and Monitoring Process Not Fully Developed

In general, quality assurance surveillance plans should be prepared in conjunction with a contract's statement of work. The plans should specify all work requiring surveillance, and the method of surveillance. NARA had prepared the Standard Operating Procedure (SOP) for TIC SLA Monitoring. However, it did not include the designation of the monitoring duties to specific individuals or offices. According to the DARs for the contract, the monitoring duties had not been formally assigned and communicated. We also found that, although the contractor started providing the TIC service for NARA in July 2011, a number of the key IT Security staff at NARA, including the Chief Information Security Officer (CISO and Deputy CISO, had not visited the contractor's data centers, network operations center (NOC), or security operations center (SOC) for contract oversight purposes.

According to the CISO, NARA had been relying heavily on the fact the contractor was a vendor approved by GSA, and Networx is a GSA-managed contract. However, the contract indicates it is the subscribing agency's role to provide oversight for the contractor's performance. Further, the lack of a complete and comprehensive contract monitoring process resulted in incomplete information on the Monthly Compliance Reports, and unmet Service Level Agreements (SLAs) going undetected and undisputed (more details are discussed in **"Monthly Compliance Reports are Not Fully Reviewed"** below).

Furthermore, there is a worksheet called a "SAN-TAN (Storage Area Network – Tape Area Network), which describes the server backup and tape storage procedures specific to each subscribing agency. A copy of the worksheet should be available via NARA's DARs. However, neither the DARs nor the IT Specialist who was involved in the installation process was familiar with the worksheet, and neither could provide a copy. According to the CISO, there was also a Memorandum of Understanding (MOU) between NARA and the contractor which described the security incident alerting rules. Although we contacted a number of individuals including the CISO, NARANet ISSO, and a DAR for the contract, none of the individuals were able to locate and provide a copy of the document. We also noted that network-based intrusion prevention is not enabled for NARA's network environment. However, NARA's Senior IT Security Specialist was not aware it was not enabled. According to the IT Specialist involved in the TIC installation, there was additional cost associated with enabling intrusion prevention and NARA chose not to receive the service. However, this information was not properly communicated to key IT Security staff.

Moreover, there was an event in May 2013 with the attributes [redacted] According to the NITTSS Security Team Lead, the attack [redacted] and was thwarted by the TIC provider's UTM device. However, per inspection of the screenshot including the rule set for the [redacted]

Monthly Compliance Reports Not Reviewed in Full

According to the GSA Networx Service Level Agreement (SLA) Management Guide, GSA recommends agencies review the Agency-Specific SLA Monthly Compliance Reports. The agency can then identify discrepancies between the contract-required performance target and the actual performance, apply for credit within six months, ensure receipt of SLA credit within two billing cycles, and escalate any unresolved SLA issue to GSA.

From January through December 2012, efforts were made to review the Monthly Compliance Reports, along with other internal reports, and submit credit requests for network outage incidents. However, information on the reports for other services had not been reviewed for completeness and accuracy, resulting in: (1) undetected missing actual performance values for a product for the entire period reviewed; and (2) unapplied SLA credits for at least two instances.

"MTIPS – Transport Collection and Distribution" is a product listed on the Monthly Compliance Reports, where the contractor's performance and availability of security incident reporting to US-CERT are measured. We found the actual availability and performance data were not included on the reports for the entire period reviewed (December 2011 was the last month where the actual data were included on the report). According to the contractor, the data was missing due to an issue with the contractor's database inventory which led to a failure to automatically populate the data on the reports. However, NARA had not contacted the contractor regarding the missing data so the reports could be corrected. NARA currently does not have any other mechanism to measure if the contractor's security incident reporting was performed or made available within the Acceptable Quality Levels (AQLs). Therefore, not reviewing this section of the reports resulted in potential loss of SLA credits and inability to confirm whether security incident reporting was performed in accordance with contract requirements.

Additionally, the contractor's actual performance values for other products had not always met the AQLs. However, NARA had not been actively reviewing the reports for all unmet AQLs, nor had they developed a process to identify the cause of and solution for the unmet AQLs. As a result, corresponding SLA credit request forms were not submitted for those unmet AQLs. At least one of the Key Performance Indicators (KPIs) pertinent to security of the network had not met the AQL for two consecutive months during the period reviewed. In April and May 2012, the KPI "Event Notification" for medium priority under the Managed Firewall Service had actual performance values of 7.25 hours and 5.50 hours, respectively, which were not within the AQL of 4.0 hours. According to the contractor, this KPI is defined as the time taken between the detection of an event from the firewall and reporting the event to the subscribing agency. Reporting firewall events to the agency within the AQL is essential to securing NARA's network environment and data because it enables timely analysis and resolution of the incident before further harm is done to the network. In addition, credit requests for these unmet SLAs were not made, and the Designated Agency Representatives (DARs) were not able to provide specific information on how to submit a credit request for this type of unmet AQL, or what credit amount would be due to NARA.

According to the Networx SLA Management Guide, if the contractor fails to meet any of the KPIs for an SLA for a given month, the agency is entitled to a credit of 12.5% of the Monthly Recurring Cost (MRC), and 25% and 50% of the MRC for the second and third consecutive months for which the SLA was not met. We found from the contractor's summaries of services that the MRC for Managed Firewall Service for the months of April and May 2012 was $2,056.55. Thus the credit amount for these unmet SLAs is estimated to be $2,056.55 x (12.5% + 25%) = $771.21, which could have been put to better use. Also, NARA might have been entitled to potential, additional credit if: (1) the actual performance values of the MTIPS – Transport Collection and Distribution SLA were properly populated on the Monthly Compliance Reports; (2) NARA had been reviewing the Monthly Compliance Reports and monitoring the contractor's performance on the SLA; and (3) any unmet AQLs were identified and notified to the contractor. However, as the actual performance values for the SLA were not included on the Monthly Compliance Reports and NARA did not independently track the actual performance values, we were unable to determine the amount of the potential lost credit.

Recommendations

We recommend NARA's Chief Information Officer:

5. Develop a comprehensive quality assurance surveillance plan that includes the services provided by the contract, surveillance methods for each service, and designation of the surveillance/monitoring duties to appropriate individuals or offices.
6. Develop a comprehensive method to verify that the actual performance data included on the contractor's Monthly Compliance Reports is complete and accurate for each service provided by the contractor.
7. Develop a comprehensive process to ensure SLA credits are requested in a timely manner by designated individuals at NARA, and to verify whether the amount of credit received is accurate based on the SLA type and number of consecutive months the SLA miss occurred.
8. Request corrected Monthly Compliance Reports including the actual performance values for all services NARA procured from the contractor for the last six months, review the reports to determine whether there were any unmet SLAs for which NARA would be entitled to a credit, and request the identified credit(s), if any, in accordance with the contract.
9. Create a process to ensure information pertinent to performance of the contract, including agreed-upon procedures for securing the network, is properly communicated to and from the contractor and among the individuals at NARA whose job responsibilities require attention to such information.

10. Perform a cost-benefit analysis for enabling the intrusion prevention option for the network-based IDPS.
11. Evaluate the rule sets of the IDPSs for NARA's network on a periodic basis to ensure proper rules have been selected and enabled to effectively detect and prevent intrusive attacks.

Management Response

Management concurred with the recommendations.

3. Improvement is Needed on Incident Response, Reporting, and Training

Overall, NARA's computer incident response and reporting appeared to be operating effectively. NARA's Computer Incident Response Team (CIRT) and the TIC provider's Security Operations Center (SOC) make collective efforts to detect, prevent, resolve, and report computer security incidents. We judgmentally selected a sample of 80 security incidents opened from October 2011 through October 2012. We then reviewed the incident reports in NARA's incident management system, email communications from/to US-CERT regarding the incidents, and made inquiries as necessary with the NARANet ISSO to obtain more details on the incidents. The majority of the computer security incidents sampled were entered in the incident management system and brought to the CIRT's attention in a timely manner, correctly categorized into the US-CERT-specified incident categories, and resolved through the appropriate resolution process.

Opportunities for improvement do exist in the management and monitoring process for incident response, reporting incidents to US-CERT, and providing the CIRT team with internal and/or external training on incident response. We also found control enhancement is needed to appropriately handle paper disclosure of personally identifiable information (PII). The following are issues we identified in these areas, which are discussed in more detail in the next sections:

1) 60 of the 80 sampled incidents (75%) were not reported to US-CERT within the specified timeframes.
2) The resolution process for a number of incidents included unjustified time gaps ranging from one month to over one year.
3) Incident response training and exercises had not been conducted on a periodic basis to keep the staff up to date with the most recent patterns of cyber attacks and remediation methodologies.

4) In case of a paper PII disclosure, there is no process ensuring copies of the documents containing PII are properly disposed of or returned.

These issues existed because the policies and procedures on incident response, reporting, and training are not clearly defined, effective, or properly followed. As a result, NARA may be at risk of: (a) not being able to promptly and effectively resolve and/or report incidents to minimize the impact within the Agency and across the government environment; and (b) allowing inappropriate access to and use of the PII disclosed to an unintended user.

Untimely Reporting of Incidents to US-CERT

US-CERT specifies the timeframes within which a computer security incident should be reported to US-CERT. They vary between one hour and one month from discovery, depending on the category and severity of the incident. For example, Category 3, Malicious Code events should be reported daily or within one hour of discovery if the event is widespread across the agency. Reports of computer incidents should include a description of the incident or event using the appropriate taxonomy. They should also include as much of the following information as possible: agency name, point of contact, incident category type, incident date and time, source and destination IPs, and operating system. However, reporting should not be delayed to gain additional information.[10]

Of the 80 sampled incident reports and their corresponding email communications from/to US-CERT, only 19 incidents were reported to US-CERT within the specified timeframes. These were comprised of Categories 3, 4, and 5 incidents and Disclosure of PII.[11] Only one of the 61 Category 3, Malicious Code events in the sample was reported to US-CERT within the suggested 24 hours of discovery. Of the rest, 58 incidents were reported between two and 39 days past the timeframe, one incident was reported 158 days past the timeframe, and one incident was re-categorized into a non-reportable event. Also, there was one incident initially categorized as a Category 6, non-reportable incident, which was then re-categorized into Category 3. This incident was then reported 398 days past the suggested timeframe for Category 3 incidents. Overall, the late reporting was caused by one or more of the following:

[10] http://www.us-cert.gov/government-users/reporting-requirements

[11] Disclosure of PII events are reported to US-CERT using various incident categories depending upon the nature and method of the disclosure. Our sample contained a total of 14 PII disclosure incidents, and one of the incidents was a computer-based, Category 4 incident and the rest were paper-based, Category 6 veteran/civilian PII disclosure incidents caused by sending incorrect documents to the recipients.

1) The incident resolution process had a lag time between steps (for example, from completion of malware scanning on the infected machine to re-baselining it to the original state and/or from resolution of the incident to reporting it to US-CERT).
2) NARA generally attempted to gather more comprehensive information about the incident before the report was sent to US-CERT.
3) Security incident tickets, opened and closed, had not been reviewed on a regular basis to determine whether appropriate actions had been taken to successfully resolve the incident and report it to US-CERT in accordance with the guidelines.

For example, for the incident reported 158 days past the suggested timeframe, we found it was first submitted into the incident management system on February 23, 2012, for a potentially infected workstation. The vulnerability assessment was not completed until March 9, 2012. Then there was an approximately 3-month gap between the date of vulnerability assessment completion, and scheduling of a re-baselining of the workstation on June 19, 2012. The NARANet ISSO was unable to recall what happened between these two dates. In addition, another gap existed between the completion of re-baselining the workstation and reporting it to US-CERT, which was not done until July 31, 2012.

Another example reviewed was from an incident initially categorized as a non-reportable, Category 6, Investigation event which was later re-categorized into a Category 3, Malicious Code event, according to the NARANet ISSO.[12] This event was detected and brought to NARA's attention by the Security Operations Center of the TIC contractor on November 7, 2011, and involved [redacted] Although the host was scanned for viruses, re-imaged, and redeployed within three days of the initial detection, the incident was not reported to US-CERT until December 10, 2012, which was 398 days past the suggested reporting timeframe for Category 3 incidents. According to the NARANet ISSO, this occurred because the helpdesk technician incorrectly closed the incident ticket, which was reopened during a review of the open and resolved security tickets.

US-CERT's mission is to improve the nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risk to the nation. As such, untimely reporting of the incidents may prevent US-CERT and other investigative agencies from promptly investigating the incident to minimize the impact across the government environment.

[12] The list of the incident reports provided did not reflect the later re-categorization; therefore, this remained as a Category 6 incident in our sample.

Training and Exercises Not Provided on a Periodic Basis

NARA's Enterprise Architecture requires that the NARA system owner or ISSO shall train personnel in their incident response roles and responsibilities with respect to the information system, and provide refresher training at least annually. According to NIST Special Publication 800-61 Rev. 2, the incident response team members need much broader knowledge than most IT staff members because they work with many facets of IT, and they must understand how to use the tools of incident response. In Mandiant's Incident Response Program Enhancement Gap Analysis conducted in 2010, Mandiant found several members of the NARA group had indicated they do not have a consistent approach to addressing incidents from one person to another. Instead, the individuals' knowledge dictated how each person would approach any particular investigation. Mandiant recommended one or more simple exercises should be scheduled to allow the participants to practice collecting data, analyzing data, and developing a recovery/remediation plan.

We found that, although it is required in NARA's Enterprise Architecture, the annual training or exercises on incident response had not been provided to the individuals who perform or support computer security incident handling. According to the Senior IT Security Specialist, the last exercise on incident response was conducted by Mandiant in June 2010, and other in-house exercises had not been conducted since then. This occurred because, although there is a policy to conduct the training on an annual basis, the process to ensure the trainings and exercises are conducted as required had not been established. Further, according to the CISO, although most CIRT members occasionally attend external training to maintain their certifications, there is no formalized policy at NARA requiring CIRT members attend training on matters related to cyber attacks and remediation measures.

As cyber attacks evolve and the patterns of attacks change over time, it is important to ensure the individuals performing intrusion detection and incident response are adequately trained on how to detect and handle the incidents more effectively and efficiently. Failure to keep the staff updated, refreshed, and trained on the attack/incident types/patterns and handling them may result in: (1) a potential attack going undetected or only partially detected; and (2) the detected attack not being mitigated fully and timely before it has substantial impact to the host(s) and network. [redacted]. According to the CISO, NARA's network-based intrusion detection system NIDS provided by the TIC contractor [redacted]

[redacted] Later, Mandiant was contracted to perform a threat assessment for the APT events and discovered [redacted]

Recommendations

We recommend NARA's Chief Information Officer:

12. Ensure the preliminary reporting of all incidents and events reportable to US-CERT is made within the US-CERT-specified timeframes. Further details on the incident or event gathered after the original reporting should be communicated to US-CERT as an update, rather than delaying the original reporting to gather information.
13. Ensure the resolution process for a computer incident is appropriately monitored and reviewed on a timely and periodic basis to minimize erroneously closed incident tickets and the unnecessary time gaps between the resolution steps.
14. Ensure incident response tabletop exercises are conducted for staff performing and/or supporting computer security incidents on at least an annual basis, and practical and relevant topics to NARA's computing environment are covered within the exercises.
15. Develop a policy for CIRT members to take training at least on an annual basis to ensure they remain up to date with current patterns/types of cyber attacks and effective, efficient incident remediation methodologies.

Management Response

Management concurred with the recommendations.

4. Physical Security of the IDS Devices Needs Improvement

During this audit, we visited three data center/computer room facilities including the computer room at Archives II, and two of the TIC contractor's data centers in Sterling, VA, to observe the physical security of the intrusion detection and prevention devices. The management server and database server for the centralized HIPS and anti-virus management system were hosted in the computer room at Archives II, and the inner and outer firewalls for the network were located in the contractor's data centers, one in each location. To assess the physical security and environmental safety controls for these facilities and the IDS devices in them, we primarily used the controls found in NIST Special Publication 800-53. In addition, we used SANS Institute's Data Center Physical Security Checklist, dated December 1, 2001, as a reference to determine the controls to be assessed for each data center facility. For the contractor's data centers, we reviewed a

number of reports prepared by third-party independent assessors, including DHS's CyberSecurity Capability and Compliance Validation reports and the SSAE No. 16 Type II reports prepared by an independent public account firm. Inquiries were also made with both the NARA and contractor individuals to obtain necessary information and supporting documents.

The physical security and environment controls at the contractor's data centers appeared to be adequately designed and operating effectively in accordance with NIST Special Publication 800-53 in areas including: (1) securing monitoring the centers and the IDS devices; (2) physical access authorization and review; (3) visitor access controls; (4) fire suppression and water leakage controls; (5) temperature and humidity controls; and (6) storage of backup tapes. NARA also had some excellent controls in securing and safeguarding the computing equipment within the computer room at Archives II including the use of locked cabinets for its computer equipment, monitoring of the computer room through surveillance cameras, temperature and humidity controls, and fire suppression. However, we noted opportunities exist to better secure and safeguard NARA's computing equipment from inappropriate access, destruction, theft, or unavailability. Specifically, the following conditions exist for the Archives II computer room, and are expanded upon below:

- The physical access list is not reviewed on a periodic basis.
- The visitor log is not reviewed on a periodic basis.
- Cables within the cabinets are poorly organized and unlabeled.

These conditions exist because NARA had not always followed the policies documented in the Enterprise Architecture, the security controls recommended in NIST Special Publications including 800-53, or the specific policies and procedures for certain controls had not been fully developed and documented. As a result, NARA's computing equipment in the Archives II computer room may be at risk of: (1) inappropriate and unauthorized use; and (2) theft, destruction, damage, or unavailability.

Physical Access Review Not Performed on a Periodic Basis

NARA's Enterprise Architecture states, in accordance with the Physical and Environmental Protection (PE) control family of NIST Special Publication 800-53, that the NARA Space and Security Management Division shall review and approve the physical access list and authorization credentials. Personnel no longer requiring access are to be removed. This must be done within the frequency defined in the System Security Plan (SSP) for unclassified information systems, or at least annually for classified information systems. According to the NARANet ISSO, although the physical

access review has been performed at least annually since 2010, there is no documented process for conducting the review. Based on the supporting documents provided, the two most recent reviews prior to this audit were conducted in August 2010 and March 2011. Another review was conducted during this audit in November 2012, as a response to our request for a copy of the physical access list. In this review, management found three individuals who were granted access to the computer room by clerical errors.

NARA's centralized HIPS and anti-virus management system is an unclassified subsystem within NARANet, according to the NARANet ISSO. Although NARA's Enterprise Architecture requires physical access reviews within the frequency defined by the SSP, the SSP for neither the NARANet GSS Application Servers nor the Common Controls defined the frequency. Not having documented, specific procedures for reviewing the physical access list may lead to: (1) failure to review the list on a regular basis; (2) access granted due to clerical or systematic errors going undetected; (3) individuals no longer requiring access not being removed from the list in a timely manner; and (4) data damage, loss, or manipulation caused by (2) or (3) above.

Visitor Log Not Reviewed

NARA's Enterprise Architecture states, in accordance with the Physical and Environmental Protection (PE) control family of NIST Special Publication 800-53, the NARA Space and Security Management Division shall review visitor access records. This must be done within the SSP-defined frequency for unclassified information systems, and at least every 90 days for classified information systems. NARA maintains a visitor log book at the front desk of the computer room at Archives II. However, the SSP for neither the NARANet GSS Application Servers nor the Common Controls defined a frequency for review of the log. According to the NARANet ISSO, there is not a process to review visitor logs periodically.

As of December 4, 2012, there were 26 entries filled out by the visitors from July 21, 2012 through December 3, 2012. However, not all of the entries included all the required information. For example, three entries were missing the dates of visits, seven were missing a NARA contact person, four were missing the NARA organization, 13 were missing reasons for the visits, and seven were missing the exit times. Additionally, although the log book instructs visitors to include detailed reason for the visit and not to write "work," 10 of the entries only included generic descriptions as "server" or "service." Incomplete and/or inaccurate information regarding the visit may lead to less auditability in the event of unauthorized or inappropriate access to the equipment and any consequences, including destruction or removal of the equipment and data spoilage.

Improvement Opportunities in Cable Management

NIST Special Publication 800-53 recommends employing clearly identified and physically separated cable trays as a control enhancement to protect against unauthorized physical connections. The Network Discovery and Assessment Report completed by IMRI in August 2012 revealed NARA did not tag cables so that the network administrator would be able to determine the source and destination of every cable attached to a switch or server. We inspected the back of NARA's centralized HIPS and anti-virus management database servers and found the cables connected to the servers were unlabeled and poorly organized without any cable ties (see **Figure 1: Back of the HIPS and anti-virus Management and Database Servers** below). The unlabeled and poorly organized cables may result in: (1) diminished productivity by not being able to quickly identify the source and destination of each cable; (2) damage to the cables causing unavailability of the service; and (3) the cables being frayed, exposing energized wires, causing a fire hazard.

Figure 1: Back of the HIPS and Anti-virus Management and Database Servers

Recommendations

We recommend NARA's Chief Information Officer:

16. Fully develop and document a process for reviewing the list of individuals with access to systems hosted in NARA's computer rooms, define the frequency of the review in accordance with system categorization and availability requirements, and ensure the frequency is properly documented in the system's SSP.
17. Fully develop and document the process for reviewing visitor logs for NARA's computer rooms, including clearly defined review frequencies and assignment of the duties to appropriate individuals for performing, reporting, and acting upon the review (when corrective/investigative actions are needed).
18. Fully develop and document the policies and procedures for a cable management system, including labeling, using proper cable ties and/or trays, and periodic inspection of the cables, for the HIPS and anti-virus management system.

Management Response

Management concurred with the recommendations.

Appendix A – Acronyms and Abbreviations

AC	Access Control
APT	Advanced Persistent Threat
AQL	Acceptable Quality Level
CIRT	Computer Incident Response Team
CISO	Chief Information Security Officer
CMRS	Case Management and Reporting System
COTS	Commercial Off-the-shelf
DoS	Denial of Service
DDoS	Distributed Denial of Service
DHS	Department of Homeland Security
ERA	Electronic Records Archives
GSA	United States General Service Administration
GSS	General Support Services
HIPS	Host Intrusion Prevention System
HTTPS	Hypertext Transfer Protocol Secure
IA	Identity and Authentication
IDS	Intrusion Detection System
IDPS	Intrusion Detection and Prevention System
IP	Internet Protocol
IPS	Intrusion Prevention System
ISSO	Information System Security Officer
KPI	Key Performance Indicator
MPLS	Multiprotocol Label Switching
MTIPS	Managed Trusted Internet Protocol Service
NARA	National Archives and Records Administration
NIDS	Network-based Intrusion Detection System
NIST	National Institute of Standards and Technology
NITTSS	NARA Information Technology and Telephone Support Services
NOC	Network Operations Center
NPRC	National Personnel Records Center
OFAS	Order Fulfillment and Accounting System
PE	Physical and Environmental Protection
PII	Personally Identifiable Information
RCPBS	Records Center Program Billing System
SLA	Service Level Agreement
SOC	Security Operations Center
SSP	System Security Plan
TCP	Transmission Control Protocol
TIC	Trusted Internet Connections
US-CERT	United States Computer Emergency Readiness Team
UTM	Unified Threat Management
VLAN	Virtual Local Area Network

Appendix B - Management's Response to the Report

NATIONAL ARCHIVES

Date: SEP 05 2013

To: James Springs, Acting Inspector General

From: David S. Ferriero, Archivist of the United States

Subject: DRAFT OIG Report 13-12, Audit of NARA's Intrusion Detection and Prevention Systems and Incident Response (IDS)

Thank you for the opportunity to review the subject draft report. We appreciate your time in reviewing our informal comments and making some clarifying adjustments.

We concur with each of the 18 recommendations and will address them further in our action plan. If you have any questions about this response, please contact Mary Drak at 301-837-1668 or at mary.drak@nara.gov.

DAVID S. FERRIERO
Archivist of the United States

NATIONAL ARCHIVES *and*
RECORDS ADMINISTRATION
8601 ADELPHI ROAD
COLLEGE PARK, MD 20740-6001
www.archives.gov

Appendix C - Report Distribution List

Archivist of the United States
Deputy Archivist of the United States
Chief Information Officer
Chief Operating Officer