AUDIT OF NARA'S COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FY 2007

OIG Report No. 08-05

March 20, 2008

AUDIT OF NARA'S COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR 2007

TABLE OF CONTENTS

CHAPTER **PAGE**

EXECUTIVE SUMMARY

Information and the systems that process it are among the most valuable assets of any organization. Adequate security of these assets is a fundamental management responsibility. The Federal Information Security Management Act (FISMA) sets forth a comprehensive framework for ensuring the effectiveness of security controls over information resources supporting federal operations and assets.

FISMA requires the head of each agency to: (a) provide information security commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency; and information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency; and (b) ensure senior agency officials provide information security for the information and information systems supporting the operations and assets under their control. Furthermore, FISMA requires the Office of Inspector General (OIG) to annually evaluate the agency's information security program and report to OMB.

As part of the annual FISMA review we conducted an audit this year instead of an evaluation. We assessed the adequacy of controls over information security and compliance with information security policies, procedures, standards, and guidelines. Specifically, we determined the effectiveness of the NARA information security program by testing the information security policies, procedures, and practices over a representative sample of the agency's systems.

Some of the weaknesses we identified in our audit have been identified in previous FISMA evaluations and in Audit Report 06-09 "Review of NARA's Information Security Program," July 31, 2006. We continued to find significant weaknesses that can be attributed to deficiencies in the design and operation of internal controls within the Office of Information Services (NH). Due to the significance of these weaknesses NARA cannot be assured its systems and data are adequately secured. As a result, information technology (IT) security is a material weakness within NARA.

Specific weaknesses identified this year include:

a) Incident detection, reporting, and response capabilities at NARA were not adequate to ensure incidents were detected quickly, fully investigated and resolved, and reported to appropriate officials, if needed. In addition, NH officials did not follow documented procedures and did not test their incident handling and response procedures during the year. Without adequate incident handling capabilities, NARA cannot rapidly detect computer-security related incidents, minimize loss and destruction, mitigate exploited weaknesses, and quickly restore computing services.

b) IT systems were not appropriately certified and accredited for operation. Specifically, NH officials did not properly complete many of the detailed activities required for certification and accreditation. Without a proper certification and accreditation (C&A) of systems, NARA lacks assurance that its systems and data are secure. In addition, certifying and accrediting officials may not have had sufficient information to make timely, credible, risk-based decisions on whether to authorize operation of those systems.

c) Of the 12 systems reviewed, 7 systems were identified as critical to NARA's mission. However, a recovery strategy was not defined in the contingency plans for these systems. Without a recovery strategy for its mission critical systems, NARA does not have assurance critical systems can be recovered within necessary time periods.

d) Standardized test procedures were used to test aspects of the contingency plans, however, the tests did not actually test the feasibility of the plan or determine whether effective communication would occur between contingency plan participants. By not testing the contingency plans, NARA does not have assurance the plans can be implemented quickly and effectively in the event of a disaster.

e) NH officials did not establish a formal process to manage, prioritize, and track IT security weaknesses identified in the NARA Information Security Program. Specifically, the program-level plan of action and milestones[1] (POA&M) did not include all IT security weaknesses and vulnerabilities known to management. Without a complete POA&M, the Chief Information Officer (CIO) may not have proper visibility of IT security weaknesses and can not use the POA&M as an effective management tool to request and allocate resources for correcting IT security weaknesses.

f) Only 35 of the 67 (52%) individuals with significant security responsibilities completed the additional level of security awareness training and IT contractors were not required to complete the additional training even though they have significant security responsibilities over NARA IT assets and are IT security professionals. The NARA Managers and Information System Security Officer training course was intended for those individuals whose jobs involve significant security responsibilities associated with the management or technical oversight of NARA IT systems. The purpose of the course was to provide current information about changes in IT security doctrine and reference policy and guidance affecting IT security programs. Failure to ensure employees receive training at a level associated with their responsibilities at NARA increases the risk of security breaches resulting from employees who are not fully aware of their security roles and responsibilities.

[1] A plan of action and milestones, also referred to as a corrective action plan, is a tool identifying tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones. The purpose of the POA&M is to assist agencies in identifying, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems.

g) Privacy Impact Assessments[2] (PIAs) did not contain all the information required by OMB 03-22 *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 30, 2003. Information omitted related to how the personally identifiable information in the system would be secured and what choices were made as a result of performing the PIA. Without this information the public, whose information may be stored in the system, does not have assurance their information is being properly protected.

In addition, an internal program review[3] funded by NH during FY 2007 determined that NARA's information security policies lacked clearly defined responsibilities and actions and did not have a mechanism in place to monitor the policies and procedures. Strengthening management controls over the information security program by revising policy and procedures and then enforcing compliance with the procedures will help to ensure control weaknesses are corrected and NARA complies with applicable laws and regulations in the future.

We made 21 recommendations that, when implemented, will assist the agency in establishing an information security program meeting FISMA and NIST requirements.

[2] A privacy impact assessment is a process for examining the risks and ramifications of using IT to collect, maintain, and disseminate information in identifiable form from or about members of the public, and for identifying and evaluating protections and alternative processes to mitigate the impact to privacy of collecting such information.

[3] The Program Review for Information Security Management Assistance Report, October 30, 2007.

INTRODUCTION

BACKGROUND

FISMA directs each Federal agency to develop, document and implement an agency-wide information security program to protect the information and information systems supporting the operations and assets of the agency. According to FISMA, the head of each agency is responsible for providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency; and information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. In addition, the head of each agency is responsible for ensuring senior agency officials provide information security for the information and information systems supporting the operations and assets under their control.

FISMA directs the head of each agency to delegate to the agency CIO the authority to ensure compliance with FISMA requirements including: (a) developing and maintaining an agency-wide information security program; (b) developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements; (c) training and overseeing personnel with significant responsibilities for information security; and (d) assisting senior agency officials concerning their responsibility to provide information security.

NARA Directive 101, Part 3 "Office of Information Services," September 30, 2007, appoints the Assistant Archivist of Information Services as the NARA Chief Information Officer (CIO). The CIO is responsible for leading the NARA-wide information technology (IT) program to carry out the provisions of the Information Technology Management Reform Act of 1996 and the E-Government Act of 2002. The CIO also ensures the NARA IT program conforms to all NARA and Federal standards, policies, and guidelines for interconnectivity and interoperability, computer system efficiency, and computer security.

In accordance with Office of Management and Budget (OMB) Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, agencies are required to establish controls to assure adequate security for all information processed, transmitted, or stored in Federal automated information systems. "Adequate security" means security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to, or modification of, information. This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls.

OBJECTIVES, SCOPE, AND METHODOLOGY

The overall objective of the audit was to assess the adequacy of controls over information security and compliance with information security policies, procedures, standards, and guidelines. Specifically, we determined the effectiveness of the NARA information security program by testing the information security policies, procedures, and practices over a representative sample of the agency's systems.

The audit was conducted at Archives II in College Park, MD with the Office of Information Services (NH) and the Office of General Counsel (NGC).

To accomplish our objective, we reviewed Public Law 107-347, the Federal Information Security Management Act of 2002, OMB Circular A-130, NIST standards and guidance as well as OMB policy memoranda. We interviewed NH and NGC officials and reviewed documentation provided by those offices to determine whether NARA has adequate controls to ensure compliance with FISMA and other Federal policy requirements. Specifically, we obtained an inventory of information systems from the CIO and selected a representative judgmental sample to review. For the 12 systems selected as part of the sample, we obtained and reviewed: certification and accreditation documents; contingency plans; documentation of tests of security controls performed; risk and/or threat assessments; system security plans, Plan of Action and Milestones; and any additional documentation needed to answer the audit objective. In addition, we obtained and reviewed the privacy impact assessments to determine whether all information required by OMB 03-22 was included.

This performance audit was conducted in accordance with generally accepted government auditing standards (GAGAS) between June 2007 and January 2008. These 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.

COMPUTER SECURITY INCIDENT RESPONSE CAPABILITY

FISMA requires each agency to implement an information security program that includes procedures for detecting, reporting, and responding to security incidents. Security incidents[4], whether caused by viruses, hackers, or software bugs, are becoming more common. When faced with a security incident, an agency should be able to respond in a manner that both protects its own information and helps to protect the information of others that might be affected by the incident. To address this concern, agencies should establish formal incident response mechanisms.

According to NIST SP 800-61 *Computer Security Incident Handling Guide,* January 2004, computer security incident response has become an important component of information technology (IT) programs. Security-related threats are not only more numerous and diverse but also more damaging and disruptive. New types of security-related incidents emerge frequently. Preventative activities can lower the number of incidents, but not all incidents can be prevented. An incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating exploited weaknesses, and restoring computing services.

NH established a computer security incident handling and response capability, the stated purpose of which was to ensure computer security incidents are identified, reported, and corrected as effectively and quickly as possible. This process, as described in NARA's *Computer Security Incident Handling Guide*, is designed to detect and respond to computer security incidents as they occur, to assist in preventing future incidents from occurring, to develop necessary response mechanisms to deal with incidents, to support IT security controls, and to implement appropriate response procedures. The guide provides guidelines for incident handling, particularly for analyzing incident-related data and determining the appropriate response to each incident.

NARA's incident handling and response capability is outsourced to two different contractor groups. Contractors for NHI (Security) are responsible for monitoring the intrusion detection system[5] (IDS) and creating trouble tickets for events identified by the IDS. Separate NHT (Operations) contractors are responsible for responding to the trouble tickets and investigating security events. A government employee was designated as the NARA Computer Incident Response Team (CIRT) Team Lead and directed the operations of the two contractor groups. The Team Lead was also responsible for the actual conduct of the incident response process and reporting incidents to the US Computer Emergency Readiness Team (US CERT)[6].

[4] According to NIST SP 800-61, a computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices.

[5] An intrusion detection system is software that looks for suspicious activity and alerts administrators.

[6] US CERT is a partnership between the Department of Homeland Security and the public and private sectors. Established in 2003 to protect the nation's internet infrastructure, US CERT coordinates defense against and responses to cyber attacks across the nation. The organization interacts with federal agencies, state and local governments, industry professionals, and others to improve information sharing and incident response coordination and to reduce cyber threats and vulnerabilities.

Continuous Monitoring of the IDS did not Exist

Continuous monitoring of the IDS did not exist during the workday to rapidly detect and respond to incidents. NH officials accepted the risk presented by a lack of 24 hour/7 day incident response however, NH officials were not aware the IDS was not continuously monitored during the workday. According to NIST SP 800-61, the longer an incident remains undetected, the greater the potential for damage and loss. Without continuous monitoring of the IDS, the response team would not be notified to begin their investigation until hours or in the case of weekends, days, after an event had occurred.

Although the CIRT Team Lead believed the IDS was continuously monitored during the workday, the IDS analyst ran only one report per day at 9:00 am compiling all the events detected from the previous 24 hours. In one example, the NARA Intrusion Detection Report for October 31, 2007, found five incidents of potentially malicious activity. Two of the incidents occurred the previous day, October 30, 2007, at 11:34 am however, because the events occurred after 9:00 am on October 30th, these events were not reported or investigated until 24 hours later.

According to NIST SP 800-61, larger organizations as well as smaller ones supporting critical infrastructures, usually need incident response staff to be available 24/7. This typically means incident handlers can be contacted by phone or pager, but it can also mean an onsite presence is required at all times. Real-time availability is the best for incident response because the longer an incident lasts, the more potential there is for damage and loss.

NH officials stated continuous monitoring of the IDS was in place -------------redacted, b(2)-------------------- and the Help Desk was staffed -------------redacted, b(2)----------. Therefore, they believed the maximum amount of time an attack would go unnoticed was 8 hours. -----------------------------------redacted, b(2)-------------------------------------- ---. According to an NH official, the risk presented by the lack of 24 hour/7 day incident response was an accepted risk because NH does not have funding to support 24 hour/7 day incident response. The CIO added she would like to improve security but is constrained by the budget.

As a result of the audit, NH officials took action and directed the contractor to begin submitting multiple IDS reports per day. Starting in November 2007, the IDS analyst began monitoring the IDS during the day and issuing ------------------redacted, b(2)------ -------------- to alert the CIRT team of new incidents discovered during the day. The IDS reports -------------redacted, b(2)----------------------------. -------------------------------- -------------------------redacted, b(2)--- -- --.

Recommendation 1. The Assistant Archivist for Information Services should add the lack of 24 hour/7 day incident response to the program-level plan of action and milestones and assess whether the risks presented require a reallocation of the IS security budget.

Management Comment(s)

The Assistant Archivist for Information Services concurred with the recommendation.

Security Events Were Not Always Fully Investigated

In reviewing security trouble tickets for events occurring between October 1, 2006 and November 1, 2007, we found several instances where security events identified by the IDS analyst were not fully investigated to determine whether an incident occurred. This occurred because NH officials did not monitor the contractor teams to ensure all events were investigated. In addition, NH officials did not ensure the two contractor teams were communicating effectively. According to NIST SP 800-61, it is imperative that the most suspicious activity is investigated. NIST SP 800-61 further states strong teamwork and communication are vital to effective incident handling. By not investigating events identified, NARA is unsure whether attacks were successful and if so, the extent of their harm.

For example, the following three events were not investigated to determine whether an incident occurred:

(1) On June 8, 2007, the NARA Intrusion Detection Report contained a high alert that a NARA system had accessed a potentially malicious website and should be investigated to determine whether the system was compromised. Based on the information provided by the IDS analyst, the NHT contractor was unable to determine which NARA workstation was involved. The NHT contractor attempted to follow-up with the IDS analyst to obtain additional information on the system involved, however, further information was not provided. The NHT contractor concluded that with the limited information, he was unable to investigate the issue further and closed the ticket on June 8, 2007.

(2) On June 29, 2007, another high alert was reported in the NARA Intrusion Detection Report. In this example, the NHT contractor was not able to investigate the issue based on the information provided. According to the trouble ticket work log, the NHT contractor spoke with the IDS analyst regarding the lack of information and the IDS analyst agreed to do further research using the firewall log in order to track down the actual system involved. However, the NHT contractor closed the ticket on June 29, 2007, before further information could be obtained.

(3) On August 17, 2007, the IDS identified an event classified as most likely malicious in nature. The NHT contractor responding to the ticket stated there were over 40 unique external IP addresses involved and asked for clarification. The NHT contractor assigned the trouble ticket back to the IDS analyst and requested additional information. As of November 28, 2007 this ticket status is "Work in Progress" meaning it has not been resolved or investigated.

NH officials, including the CIRT Team Lead, did not monitor the two contractor teams to ensure events were adequately investigated. Although the lack of information was communicated in the work log for the trouble tickets, NH officials did not request additional action be taken to investigate the event before closing the trouble ticket. In addition, NH officials did not facilitate interaction among the two contractor teams to try and obtain the information needed. According to the NARA incident handling procedures, the Information Security Officer is responsible for monitoring the resolution of all incidents, however, there was no evidence any monitoring took place.

In addition, NH officials did not ensure the two contractor teams were communicating effectively in the incident handling process. During the audit, we noted uncertainty by both contractor teams as to whether the other had the knowledge and skills necessary to perform the job correctly. According to NIST SP 800-61, teamwork and communication are needed for effective incident handling therefore, doubt could adversely affect the ability to work together as a team. The CIRT Team Lead needs to have an active role in fostering teamwork among the two contractor teams.

Recommendation 2. The Assistant Archivist for Information Services should establish a process to review the Remedy trouble ticket work logs daily and communicate with the CIRT team, if needed, to ensure all events are fully investigated.

Management Comment(s)

The Assistant Archivist for Information Services concurred with the recommendation.

Incident Response Procedures were not Tested

NH officials did not perform testing to ensure the CIRT would function in the most efficient and effective manner possible. This occurred because NH officials believed responding to real incidents in lieu of a test satisfied the requirement. NIST SP 800-61 recommends testing the incident response procedures so the incident response team can practice responding to large-scale incidents. By not testing the incident handling procedures, NARA lacks assurance the incident handling capability is adequate to protect NARA's computer network and information systems against computer security-related incidents.

According to NIST SP 800-61, organizations typically find it very challenging to maintain situational awareness for the handling of large-scale incidents because of their complexity. Collecting, organizing, and analyzing all the pieces of information, so the right decisions can be made and executed, are not easy tasks. The key to maintaining situational awareness is preparing to handle large-scale incidents, which should include practicing the handling of large-scale incidents through exercises and simulations on a regular basis. Such incidents happen rarely, so incident response teams often lack experience in handling them effectively.

The CIRT Team Lead stated responding to real incidents in lieu of a test satisfied the NIST requirement. However, the CIRT Team was not convened in response to any incidents during the year. Therefore, NARA has no assurance the team will function in the most efficient and effective manner possible to protect NARA's computer network and information systems against computer related incidents. Any problems associated with NARA's incident response capability need to be detected and corrected before a real, large-scale incident occurs.

Recommendation 3. The Assistant Archivist for Information Services should conduct testing of the incident response procedures involving both small and large scale security incident exercises and simulations to ensure the CIRT team functions efficiently and effectively and any problems can be identified.

Management Comment(s)

The Assistant Archivist for Information Services concurred with the recommendation.

Reporting of Computer Security Incidents was not Adequate

NH officials did not report all security incidents that occurred between October 1, 2006 and August 31, 2007, to US CERT as required. This occurred because NH officials relied on the contractor to alert them of security incidents and did not conduct reviews of the security trouble tickets opened. In addition, NH officials did not believe NARA had to follow the written procedures issued by US CERT. FISMA requires Federal agencies to report IT security incidents to the Federal Information Security Incident Center[7], a government-wide incident response capability assisting Federal civilian agencies in their incident handling efforts, within the Department of Homeland Security. As a result, NARA is not in compliance with Federal law.

We identified nine computer security incidents that were not reported to US CERT. Further, of the 15 incidents that were reported, only 4 (27%) were reported within the required timeframe.

a. At least nine incidents occurred during the year but were not reported to US CERT, as required. These incidents included one Root/User Level intrusion, two instances where malicious software was installed on NARA systems, five instances of improper usage involving the violation of acceptable computer use policies, and one incident of an attempted access.

NH officials relied on the contractors to alert them of important incidents and did not conduct reviews of the security trouble tickets opened. According to the CIRT Team Lead, his review of the security trouble tickets was limited to only those incidents

[7] The Federal Information Security Incident Center is now referred to as the US Computer Emergency Readiness Team (US CERT).

included in the daily Intrusion Detection Reports. However, by only reviewing tickets opened as a result of the IDS report, the CIRT Team Lead did not have visibility over incidents reported by the Field Operations System Administrators (FOSA) or incidents reported directly to the Help Desk by NARA users.

In one example, a FOSA identified a worm[8] that had copied itself to the local hard drive of a system and mapped itself to the network drive. The security trouble ticket was created April 13, 2007, and based on the type of incident, should have been reported to US CERT within one day. However, the CIRT Team Lead was not aware the trouble ticket had been created, or that a worm had been discovered at one of NARA's field sites until we identified the ticket during our audit. The CIRT Team Lead stated the FOSA should have alerted him regarding the discovery. However, according to the CIRT Team Lead, neither the FOSA nor the security contractor involved in investigating the incident notified him.

b. Between October 1, 2006, and September 4, 2007, NARA reported 15 computer security incidents to US CERT. In reviewing the 15 incidents reported, only 4 incidents were reported within the required timeframe because NH officials did not believe NARA had to follow the written procedures issued by US CERT. NH officials waited until August 27, 2007, or later, to report 10 of the incidents (See Table 1).

Table 1. Review of Security Incidents Reported to US CERT

Incident Category Reported by NARA	Date Identified	Date Reported to US CERT	Timeframe Required by US CERT	Submitted Within Timeframe?
1. CAT3 Malicious Logic	9/28/2006	11/7/2006	Daily	NO
2. CAT4 Improper Usage	11/16/2006	12/7/2006	Weekly	NO
3. CAT6 Investigation	unknown	3/20/2007	N/A	YES
4. CAT5 Attempted Access	4/30/2007	8/27/2007	Monthly	NO
5. CAT5 Attempted Access	5/16/2007	5/18/2007	Monthly	YES
6. CAT4 Improper Usage	5/17/2007	8/27/2007	Weekly	NO
7. CAT4 Improper Usage	5/22/2007	8/27/2007	Weekly	NO
8. CAT3 Malicious Logic	6/7/2007	6/7/2007	Daily	YES
9. CAT3 Malicious Logic	6/8/2007	8/27/2007	Daily	NO

[8] A worm is a destructive program that may destroy data or use up tremendous computer or communications resources. Worms do not replicate like viruses. Instead, worms can run independently and travel from machine to machine across network connections by exploiting vulnerabilities and application or system weaknesses.

Incident Category Reported by NARA	Date Identified	Date Reported to US CERT	Timeframe Required by US CERT	Submitted Within Timeframe?
10. CAT5 Attempted Access	6/12/2007	8/27/2007	Monthly	NO
11. CAT5 Attempted Access	6/28/2007	8/27/2007	Monthly	NO
12. CAT5 Attempted Access	6/29/2007	8/27/2007	Monthly	NO
13. CAT5 Attempted Access	7/18/2007	8/27/2007	Monthly	NO
14. CAT5 Attempted Access	7/20/2007	8/28/2007	Monthly	NO
15. CAT5 Attempted Access	7/31/2007	8/27/2007	Monthly	YES

According to NH officials, NARA's reporting processes and procedures were based off of verbal conversations with an individual at US CERT. One NH official stated actual incidents that US CERT would need to know about in a timely fashion would be reported according to the established timeframes, but because NARA's incidents were all resolved internally, NARA only had to report them by the end of year. This contradicts the written procedures published by US CERT. US CERT issued written procedures regarding the types of incidents that should be reported and established timeframes for reporting incidents, however, the NH official believed the verbal direction outweighed the written instructions.

Recommendation 4. The Assistant Archivist for Information Services should establish a process to review all Remedy security trouble tickets opened and revise the incident handling and Intrusion Detection System procedures to include the requirement that the CIRT Team Lead be notified if a high level incident is identified.

Management Comment(s)

The Assistant Archivist for Information Services concurred with the recommendation.

Preventative Control Was Not Implemented

A preventative control identified by NH officials in their FISMA response to OMB was not actually in place. This occurred because NH officials did not monitor the contractor to ensure the contractor performed the specified activities. NIST SP 800-61 states preventative activities, such as ensuring systems, networks, and applications are sufficiently secure, can lower the number of incidents. In addition, the NARA Computer Security Incident Handling Guide states preventing problems is normally less costly and more effective than reacting to them after they occur. By not ensuring preventative controls are in place, NARA may not be able to identify and fix system vulnerabilities before an attacker exploits the vulnerability.

Specifically, NH reported that as part of their testing and continuous monitoring process at least two production servers per week were audited, to include checks of the security configurations of those servers. However, when we requested the supporting documentation resulting from those audits, NH officials discovered the contractor did not perform the audits as required. Although the contractor had completed some audits, the audits were not conducted bi-weekly or on a regular basis. According to the documentation provided by NH, approximately 39 server audits were completed between June 2006 and June 2007 instead of the 104 audits which should have been completed.

In addition, NH officials did not monitor the contractor to ensure recommendations resulting from the audits were mitigated. For example:

(a) An audit conducted on an ARC server in June 2006 found ----------------------------
------------------------redacted, b(2)--

--.

(b) An audit conducted on a MILRECS server on August 1, 2006, found ----------------
----
------------------------------redacted, b(2)--

-------------------------.

(c) An audit conducted on a CMRS server on July 18, 2006, found -----------------------
----
------------------------redacted, b(2)--

--.

As of October 2007, the status of all three Change Request Tickets was "Work In Process" indicating these weaknesses have not been corrected.

NH officials did not adequately monitor the contractor to ensure the bi-weekly server audits were conducted and vulnerabilities identified were corrected. Specifically, the NH official assigned to monitor the contractor's performance was not aware of the requirement for the contractor to perform bi-weekly server audits and did not believe it was his responsibility to monitor that task because it related more to security than operations.

Recommendation 5. The Assistant Archivist for Information Services should designate an NH employee to receive the bi-weekly server audit results and to review the results to ensure procedures are followed and security vulnerabilities are mitigated in a timely manner.

Management Comment(s)

The Assistant Archivist for Information Services concurred with the recommendation.

Recommendation 6. The Assistant Archivist for Information Services should conduct a review of open Remedy tickets and direct the contractor, in writing, to address the vulnerabilities identified during the completed server audits.

Management Comment(s)

The Assistant Archivist for Information Services concurred with the recommendation.

Recommendation 7. The Assistant Archivist for Information Services should add security vulnerabilities identified during the server audits to the system's plan of action and milestones to ensure proper tracking and visibility.

Management Comment(s)

The Assistant Archivist for Information Services concurred with the recommendations.

Post-Incident Activities Were Not Conducted

NH officials did not conduct post-incident activities in accordance with NIST and NARA guidance. Specifically, post-incident activities did not include holding "lessons learned" meetings. This occurred because an NH official deleted this requirement from the incident handling procedures. NIST SP 800-61 recommends the use of lessons learned meetings to evaluate the incident handling process and identify necessary improvements to security controls and practices. By not conducting post-incident activities, NARA is missing a valuable opportunity to improve the incident handling process by identifying security weaknesses and deficiencies in the policies and procedures.

According to NIST SP 800-61, organizations should use the lessons learned process to gain value from incidents. After a major incident has been handled, the organization should hold a lessons learned meeting to review how effective the incident handling process was, and identify necessary improvements to existing security controls and practices. Lessons learned meetings should also be held periodically for lesser incidents. The information accumulated from all lessons learned meetings should be used to identify systemic security weaknesses and deficiencies in policies and procedures. Follow-up reports generated for each resolved incident can be important not only for evidentiary purposes, but also for reference in handling future incidents and in training new incident response team members.

We previously reported this finding in OIG Audit Report 06-09 "Review of NARA's Information Security Program," July 31, 2006. In that report, we recommended the Assistant Archivist for Information Services should require NARA IT security personnel to conduct post-incident activities in accordance with the guidance in NIST SP 800-61 and the NARA Computer Security Incident Handling Guide, including (1) holding "lessons learned" meetings when a major incident occurs and periodically for lesser incidents, and (2) preparing "follow-up" incident reports. Management concurred with the recommendation and agreed to take corrective action. However, the recommendation was not implemented. Instead, one NH official made revisions to the NARA Computer Security Incident Handling Guide to remove the requirement for lessons learned meetings.

A previous version of the NARA Computer Security Incident Handling Guide required post incident activities be conducted after an incident was mitigated to determine how effective the incident handling process was and to identify necessary improvements to security measures and the incident response process. An NH official, who was responsible for the actual conduct of the incident response process, made revisions to the Computer Security Incident Handling and Response Guide. According to the Revision History Table, the changes made included updating the contact lists, adding the system information system security officer contact list, changing references from FedCIRC to US-CERT and other editorial changes. However, we identified additional changes not recorded in the revision table. One revision made was to delete the requirement for lessons learned meetings. According to the NH official, he revised the incident handling guide to remove requirements NH was not following such as the post incident activities. Allowing an NH employee to revise the procedures in order to remove requirements not being followed circumvents management controls and indicates additional controls are needed in order to ensure compliance.

Recommendation 8. The Assistant Archivist of Information Services should conduct "lessons learned" meetings in accordance with the guidance in NIST SP 800-61 when a major incident occurs and periodically for lesser incidents, and develop and implement a control mechanism to verify compliance.

Management Comment(s)

The Assistant Archivist for Information Services concurred with the recommendation.

Recommendation 9. The Assistant Archivist of Information Services should revise the NARA Computer Security Incident Handling Guide to include the requirement for IT security personnel to conduct post-incident activities outlined in NIST SP 800-61.

Management Comment(s)

The Assistant Archivist for Information Services concurred with the recommendation.

Pertinent Information Missing from NARA Intrusion Detection Reports

IDS reports issued by the IDS analyst to the incident response team did not identify the date and time the event occurred. However, during a previous review of NARA's information security program, this information had been included on the IDS reports. The changes to the IDS report occurred because contractor staff changed during the year and the IDS Procedures did not require this information be included. Without the date and time the event occurred, reviews of security logs for details of the event would be extremely difficult if not impossible.

The date and time an event occurred is critical when determining which logs should be reviewed for details of the event. For example, the IDS Report dated Monday, April 9, 2007, contained two high alert events. The IDS Report did not identify which date and at what times the events occurred, making the review of logs for details of the events extremely difficult, if not impossible.

NH officials were not aware the date and time information had been removed from the IDS reports and took immediate action to begin including this information on future reports.

Recommendation 10. The Assistant Archivist of Information Services should revise the Intrusion Detection System procedures to add a requirement for the date and time of the event to be included in the daily Intrusion Detection Reports.

Management Comment(s)

The Assistant Archivist for Information Services concurred with the recommendation.

NARA CERTIFICATION AND ACCREDITATION PROCESS

Security certification and accreditation (C&A) are important activities that support a risk management process and are an integral part of an agency's information security program. According to NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004, security accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals based on the implementation of the agreed-upon set of security controls. NIST SP 800-37 further states it is essential for agency officials to have the most complete, accurate and trustworthy information possible on the security status of their information systems in order to make timely, credible, risk-based decisions on whether to authorize operation of those systems. Although NIST SP 800-37 is a guidance document, OMB has mandated the use of NIST SP 800-37 for system certification and accreditation activities.

Our review of the C&A process disclosed systems were not appropriately re-certified and accredited for operation. Specifically, NH officials did not complete many of the detailed activities required by NIST SP 800-37. Without a proper C&A of systems, NARA lacks assurance its information systems and the data they contain are secure. See Appendix A for detailed information regarding our review of systems in the sample.

The NARA IT Security C&A Methodology, version 4.6.1, September 14, 2007, states the assessment of risk and the development of System Security Plans are two important activities in an agency's information security program directly supporting C&A and are required by FISMA and OMB Circular A-130, Appendix III.

System Security Plans provide an overview of the information security requirements and describe the security controls that are either in place or planned to meet those requirements. The system security plan also delineates responsibilities and expected behavior of all individuals who access the system. The security plan should be viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system. It should reflect input from various managers with responsibilities concerning the system, including information owners, the system owner, and the senior agency information security officer. Security plans are living documents requiring periodic reviews, modifications, and milestone or completion dates for planned controls. Procedures should be in place outlining who reviews the plans and follows up on planned controls.

The plan of action and milestones (POA&M) document is a key document in the security accreditation package and identifies: (a) tasks needing to be accomplished; (b) resources required to accomplish elements of the plan; (c) milestones in meeting the tasks; and (d) scheduled completion dates for the milestones. The POA&M describes the measures that have been implemented or planned to correct any deficiencies noted during the assessment of the security controls, and to reduce or eliminate known vulnerabilities in the information security.

After a system has undergone certification and received approval to operate from the authorizing official, the system enters a “continuous monitoring” phase. “Continuous monitoring” provides oversight and monitoring of the security controls in the information system on an ongoing basis and informs the authorizing official when changes occur that may impact the security of the system. OMB Circular A-130, Appendix III requires use of the system or application be re-authorized (re-certified and accredited) every three years or whenever a significant change is made.

System Categorizations were not Properly Assigned

Overall, five systems did not have a system categorization[9] matching the availability or confidentiality requirements needed for the systems. This occurred because NH officials were not aware IT systems were mentioned in the NARA Continuity of Operations Plan (COOP) and an NH official believed the confidentiality categorizations were appropriate based on his knowledge of the systems. Federal Information Processing Standards Publication (FIPS) 199 requires agencies to categorize all information and information systems based upon the need to provide appropriate levels of information security according to a range of risk levels. As a result of not having the appropriate categorization level, information in the systems may not be adequately protected.

Specifically, three systems were identified in the NARA COOP as critical to supporting NARA’s mission, but had an availability rating of Low. Further, three systems identified as containing Personally Identifiable Information (PII) had a confidentiality rating of Low.

a. Three systems mentioned in the NARA COOP had an availability rating of Low: ---- ---------------------------------redacted, b(2)-- --. An availability classification of Low means the disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. However, because these systems are designated as essential in the NARA COOP, a disruption of access to use of the information would cause more than limited adverse effects on the organizational operations. Further, one of those three systems,---b(2)---- had an overall FIPS 199 rating of “Low.” The overall FIPS 199 rating determines the number of recommended minimum security controls for information systems. A “Low-impact” system requires fewer minimum security controls therefore, --redacted, b(2)------ may have less controls in place than the system warrants.

b. Three systems identified as containing Personally Identifiable Information had a confidentiality rating of Low: --------------redacted, b(2)------------------------------ --------

[9] NIST Federal Information Processing Standard (FIPS) 199 “Standards for Security Categorization of Federal Information and Information Systems,” February 2004, established security categories for information and information systems. The categorization is based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals.

----------------------redacted, b(2)-----------------------------. According to FISMA, confidentiality relates to preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information. Because the systems contain PII, the confidentiality level should be at least moderate.

According to NH officials, the security categorizations for systems were decided by the system owners with assistance from NH however, NH officials were not aware the NARA COOP included individual systems because NH officials had not seen the latest version of the COOP. In addition, an NH official stated two of the systems identified as containing PII did not, to his knowledge, contain PII therefore, he believed the confidentiality categorization was appropriate.

Appropriate system categorizations are important because the categorization level determines the number of baseline security controls required for the system. Therefore, by not having correct system categorizations, a system may have too many controls which would not be cost effective or, if a system was rated lower than it should be, information may not be adequately protected. NARA system owners and NH officials should review the system categorizations for these five systems to determine whether the categorization level is appropriate based on mission need and sensitivity of the data.

Recommendation 11. The Assistant Archivist of Information Services, along with the system owners, should:

a. Re-evaluate the availability requirements for -------------redacted, b(2)---, and

b. Re-evaluate the confidentiality requirements for -------------redacted, b(2)---.

Management Comment(s)

The Assistant Archivist for Information Services concurred with the recommendation.

System Security Plans and System Plans of Action and Milestones were not Complete

Of the 12 systems reviewed, 11 systems did not have a completed security plan, and the plan of action and milestones (POA&M) for 8 systems did not contain all the information required by OMB. This occurred because the CIO did not implement management controls to verify certification and accreditation activities were completed before authorizing systems to operate. FISMA Section 3544(B) requires that agencies maintain subordinate plans for providing adequate information security for networks, facilities, information systems, or groups of information systems; as well as a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in information security. As a result, NARA lacks assurance its systems and data are secure. In addition, the CIO and Chief Information Security Officer (CISO) may not have had sufficient information to make timely, credible, risk-based decisions on whether to authorize operation of those systems.

a. Eleven of the 12 systems did not have completed security plans. Generally, the systems had a portion of the information required by NIST but not all. Specifically:

(1) Ten of the 12 plans reviewed did not contain security controls tied to NIST SP 800-53 or did not describe the controls in place or planned for meeting security requirements. Federal agencies must meet the minimum security requirements defined in FIPS 200 through the use of the security controls in NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*. The controls selected or planned must be documented in a system security plan and tied to NIST SP 800-53.

(2) Nine of the 12 plans reviewed did not identify the overall FIPS 199 categorization for the system or contained inconsistent information within the plan regarding the categorization level selected. FIPS 199 defines security categories for information systems based on potential impact on organizations, assets, or individuals should there be a breach of security—that is, a loss of confidentiality, integrity, or availability. FIPS 199 requires agencies to select an overall security category for the information system using a high watermark approach[10]. Therefore, it is especially important for the overall FIPS 199 categorization to be included in the plan when there are various impact levels contained in one information system.

(3) Five of the 12 plans reviewed did not adequately define the roles and responsibilities for the system. According to NIST SP 800-18, a designated system owner must be identified in the security plan. In addition, an authorizing official and an individual responsible for security of the system must be identified in the security plan for each system.

(4) Five of the 12 plans reviewed did not contain the rules of behavior for the system. The rules of behavior, which are required by OMB Circular A-130, Appendix III, and is a security control contained in NIST SP 800-53, should clearly delineate responsibilities and expected behavior of all individuals with access to the system. The rules should state the consequences of inconsistent behavior or noncompliance and be made available to every user prior to receiving authorization for access to the system.

b. Of the 12 systems reviewed, 8 system POA&Ms did not contain information needed to track and correct security weaknesses identified in the systems. Specifically:

[10] The high watermark approach required by FIPS 199 is the maximum potential impact values for each security objective (confidentiality, integrity, and availability) from the information type's resident on the system.

(1) Six of the 12 systems did not identify corrective actions to be taken to eliminate the weakness

(2) Eight of the 12 systems did not provide an estimate of the resources required to take the corrective action

(3) Six of the 12 systems did not identify the estimated completion dates for eliminating the weaknesses. In addition, for two POA&Ms where completion dates were provided, the dates had passed and the POA&M was not updated to either report the item as completed or revise the milestones.

(4) Two of the 12 systems did not provide information about the status of corrective actions. We noted the status for all the weaknesses identified in seven of the POA&Ms was "ongoing."

According to GAO *Standards for Internal Control in the Federal Government*, November 1999, the organization's control environment provides discipline and structure as well as the climate which influences the quality of internal control. Agency management plays a key role in providing leadership in this area, especially in providing guidance for proper behavior and removing temptations for unethical behavior. According to the CIO, she was aware the system security plans were not complete and believed that one reason why the plans were not complete was due to the strict deadline she established for re-accreditation of the systems in order to get the systems removed from the OMB Watch-List.

NH officials made the decision to not fully update the system security plans because it would not be possible to complete the task within the deadline. Specifically, NH officials developed a way to circumvent controls in the C&A process by completing only basic updates to the security plans and then listing the incomplete security plan as a deficiency in the system POA&M. As a result, the system security plans were not updated and do not contain the information required by NIST SP 800-18. In addition, NH typically determines the actions to be taken and the milestone dates for completion and inputs the information into the system POA&M however, due to resource constraints and pressure to complete the reaccreditations, this information had not been updated for all systems.

Although the NARA C&A Methodology directs the information system owner to ensure that the security plan is complete and that the plan contains enough detail to evaluate the system's security, NH officials did not hold the system owner accountable for the security plan and did not review the C&A package to ensure that the system security plan or the POA&M was completed before the systems were re-certified and accredited.

The contractor responsible for the certification and accreditation packages originally recommended interim authorization to operate[11] decisions for several NARA systems

[11] According to NIST SP 800-37, an interim authorization to operate is rendered when the identified security vulnerabilities in the information system resulting from deficiencies in the planned or implemented security controls are significant but can be addressed in a timely manner. An interim authorization provides a limited authorization to operate the information system and acknowledges greater risk to the

until the weaknesses identified in the POA&Ms were mitigated. This recommendation was rejected by the Certifying Official and, without addressing the security weaknesses in the system POA&Ms, the Certifying Official had the contractor revise the certification statements to recommend authorization to operate the systems. In addition, language requiring weaknesses in the POA&M to be corrected within 180 days was removed from the certification statements. We noted that based on the Certifying Official's direction, the contractor recommended 11 systems be given authorization to operate. This decision may not have been appropriate based on the vulnerabilities identified during the C&A process and the risks presented by those vulnerabilities.

In FY 2006 NH officials identified a reportable condition regarding documentation because of the incomplete C&A documentation. During interviews, NH officials indicated documentation produced had little impact on the quality of the C&A process or information security because the documents are not used once created. System documentation produced should provide valuable information as to the security controls in place for the system, and should be viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system.

Recommendation 12. The Assistant Archivist of Information Services should develop and implement management controls to monitor and enforce compliance with NIST SP 800-37 and NARA C&A policy.

Management Comment(s)

The Assistant Archivist for Information Services concurred with the recommendation.

Limited Assurance Exists over Security Control Testing

Based on our review of the security test and evaluation results, evidence did not exist to verify the tests were actually performed to the extent detailed in the test plans. This occurred because NH officials did not have an adequate process in place to monitor the contractor's performance. FISMA requires periodic testing and evaluation of the security controls in place for agency systems. Without adequate testing, NARA lacks assurance security controls are in place and working as intended to protect its systems and data.

NH officials used contractors to perform most of the security control testing this year. According to the test plan used, several tests required the tester to examine logs and access lists, interview personnel, or verify security configurations. However, work documented in the test results did not detail the extent to which the contactor followed the written test plan, and supporting documentation reviewed by the contractor during the testing was not retained.

agency for a specified period of time. When the security-related deficiencies have been adequately addressed, the interim authorization should be lifted and the information system authorized to operate.

NH officials did not have an adequate process in place to monitor the testing performed by contractors. Instead, NH officials required the contractor to record only their name, the date the test was conducted, and whether the test passed or failed. According to an NH official, the contractor was not required to document work performed and NH officials did not review any of the tests results to verify the accuracy of the tests. The information recorded in the test results does not provide assurance the test was conducted or the results of the testing can be relied upon.

Recommendation 13. The Assistant Archivist of Information Services should develop a process to monitor the contractor's performance to verify testing was performed to the extent detailed in the test plans and review the security test and evaluation results to ensure the results are reasonable.

Management Comment(s)

The Assistant Archivist for Information Services concurred with the recommendation.

Two National Security Systems were not Accredited

Two classified national security systems continued to operate even though the systems were last accredited[12] in 1997. This occurred because NH officials did not take action to obtain an accreditation statement until 2006. The Director Central Intelligence Directive 6-3 requires an accreditation decision be re-evaluated every three years or whenever any security relevant change occurs. As a result, responsibility and accountability for the security of the system has not been accepted.

NH officials sent a memorandum to the accrediting authority at the Central Intelligence Agency (CIA) alerting the agency official the systems had not been re-accredited since the original accreditation was received in 1997. According to NH officials, they tried to locate the accrediting authority since 2001, but after September 11, 2001, CIA officials had higher priorities than the re-accreditation of NARA systems and it was not until recently that contact was re-established with the accrediting authority.

NARA continues to operate the systems even though the risks presented by the systems have not been formally accepted.

Recommendation 14. The Assistant Archivist of Information Services should develop and implement a mechanism to monitor system accreditations for NARA's National Security Systems to ensure the systems are re-certified and accredited at least every three years.

[12] System accreditation is the official management decision to permit operation of an information system in a specified environment at an acceptable level of risk based on the implementation of an approved set of technical, managerial, and procedural safeguards.

Management Comment(s)

The Assistant Archivist for Information Services concurred with the recommendation.

CONTINGENCY PLANNING/DISASTER RECOVERY

IT systems are vulnerable to a variety of disruptions, ranging from mild (e.g., short-term power outage, disk drive failure) to severe (e.g., equipment destruction, fire) from a variety of sources such as natural disasters to terrorists actions. While many vulnerabilities may be minimized or eliminated through technical, management, or operational solutions as part of the organization's risk management effort, it is virtually impossible to completely eliminate all risks. In many cases, critical resources may reside outside the organization's control (such as electric power or telecommunications), and the organization may be unable to ensure their availability. Thus effective contingency planning, execution, and testing are essential to mitigate the risk of system and service unavailability.

According to OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Information Resources, for major applications, Federal agencies should establish and periodically test the capability to perform the agency function supported by an application in the event of failure of its automated support.

According to NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002, IT and automated information systems are essential to an organization's success, therefore, it is critical the services provided by these systems are able to operate effectively without excessive interruption. Contingency planning supports this requirement by establishing thorough plans and procedures and technical measures enabling a system to be recovered quickly and effectively following a service disruption.

Recovery Strategy for Restoring Mission Critical IT Systems is Inadequate

Of the 12 systems reviewed, 7 systems were identified as critical to NARA's mission, however, a recovery strategy was not defined in the contingency plans for these systems. This occurred because a business impact analysis had not been conducted to identify critical NARA processes and NH officials did not believe there was any essential service or core business function of the agency that required restoration in any particular time period. According to NIST SP 800-34, the business impact analysis is a key step in the contingency planning process and recovery strategies are developed based on the information obtained in the business impact analysis. By not having a defined recovery strategy, NARA does not have assurance that critical NARA systems can be recovered within the time period needed.

Specifically, the contingency plans for six of the mission critical systems stated that the recovery goal was to "revert to manual processing, if possible, and restore system functionality with vendor-supplied hardware as available." However, this strategy does not provide recovery capability over the full spectrum of incidents because performing the business process using manual means is typically acceptable for only short term disruptions.

According to NIST SP 800-34, a key step in the contingency planning process is the business impact analysis. A business impact analysis correlates specific system components with the critical services they provide, and based on that information, characterizes the consequences of a disruption to the system components. Conducting this type of analysis requires input from the users and business process owners as well as other associated groups. The recovery strategy selected is based on the information identified during the business impact analysis.

According to an NH official, a business impact analysis may exist as a formal document for some systems, but most of the contingency plans are based on an implied business impact analysis done by the system owner when the security plan was written. That same NH official also acknowledged:

> "The basic of assumption of almost all the contingency plans is based on the fact that there is no essential service or core business function of the agency that requires the restoration of the system in any particular time period, the exception is NARANet, thus, there is no real need for a formal linkage between the operational aspects of the current contingency plan and a business impact analysis."

However, multiple system owners identified their systems as critical to the functioning of NARA. Therefore, system owners and NH officials need to work together to determine appropriate recovery strategies.

Although NH officials identified NARANet (NARA's general support system) as the only essential system, a recovery strategy and recovery procedures did not exist for the system. NH officials provided an NH Disaster Recovery Plan dated July 30, 2007, which states as an underlying assumption that NH needs to provide IT services for NARA in the event of a major disruption to its operational IT infrastructure and critical business process. However, the Disaster Recovery plan does not detail the procedures to be followed in order to facilitate the recovery of capabilities at an alternate site.

Federal policy and guidance requires the development and maintenance of contingency plans to provide procedures and capabilities for recovering major applications or general support systems. Without a recovery strategy for its mission critical systems, NARA does not have a corrective control in place to restore IT operations quickly and effectively following a service disruption.

We issued Management Letter 07-12, "Contingency Planning for IT Systems," on September 20, 2007, to notify the Archivist regarding the significant risk to agency operations because adequate plans did not exist, and coordination among NARA Senior Managers had not been established, to ensure IT systems critical to NARA's mission could be recovered quickly and effectively following a service disruption or disaster.

Recommendation 15. The Archivist of the U.S. along with NARA Senior Management and Information Owners should:

a. Conduct a Business Impact Analysis following the instructions in NIST SP 800-34 to identify NARA's critical business processes and the systems supporting those processes; and

b. Develop recovery strategies for at least those systems identified as critical based on the outcome of the Business Impact Analysis.

Management Comment(s)

The Assistant Archivist for Information Services concurred with the recommendation.

No Record of Reviews of, or Changes to, Contingency Plans

The contingency plans for 11 of the 12 systems reviewed had not been updated since the initial plans were created. This occurred because NH officials did not believe the contingency plans needed to be updated or that it was their responsibility to update the contingency plans. NIST SP 800-34 states that it is essential for the contingency plan to be reviewed and updated regularly to ensure new information is documented and contingency measures are revised if required. As a result, the contingency plans may contain outdated information and may not accurately reflect system requirements.

Of the 11 contingency plans reviewed[13], nine were dated 2004, and one was dated 2006. The contingency plan for NARANet was the only plan dated 2007. There were no entries in the Record of Changes section in 10 of the 11 contingency plans to support that the contingency plans were reviewed at least annually, as required by NIST guidance. According to NIST SP 800-34, the plan should be reviewed at least annually or whenever significant changes occur to any element of the plan.

According to an NH official, the current system documentation was an accurate reflection of the "as is" state of system contingency planning. The CIO stated that ideally the system owner should be responsible for the contingency plan and should know what to do and be prepared if the system was unavailable for a few days because NH cannot ensure that users for every system are prepared for a system failure. However, instead of holding the system owners accountable, another NH official directed the contractor who originally wrote the contingency plans in 2004, to review and update the plans because the NH official was fairly certain that in many of the plans, the system inventory and points of contact would be out of date.

Recommendation 16. The Assistant Archivist of Information Services should:

a. Revise the IT Security Policy to identify who is responsible for reviewing the system contingency plans and revising the plans to address changes or problems encountered during plan implementation, execution, or testing;

[13] There was one contingency plan prepared for the two classified AERIC systems.

b. Implement management controls to verify contingency plans are reviewed and updated at least annually as required by NIST SP 800-34; and

c. Update the contingency plans, if needed, and record any changes made in the Record of Changes section of the plans.

Management Comment(s)

The Assistant Archivist for Information Services concurred with the recommendation.

Contingency Plans were not Adequately Tested

Testing of the system contingency plans was not adequate and did not meet the intent of NIST guidance. Specifically, tabletop testing of the contingency plans for 10[14] of the 12 systems reviewed did not evaluate the viability of the plan procedures, determine the ability of recovery staff to implement the plan, or identify deficiencies in the plan. This occurred because NH officials believed testing the viability of the contingency plans was outside of NH's responsibility. According to NIST SP 800-34, contingency plan testing is a critical element of a viable contingency capability. By not testing the viability of the contingency plans, deficiencies within the plans cannot be identified and addressed, and NARA does not have assurance the plan can be implemented quickly and effectively in the event of a disaster.

Contractor's used a standard test plan to perform the contingency plan testing. Although the test plan included a section to test the manual or alternate procedures, the actual tests conducted did not test the manual or alternate procedures. For example, the test of the contingency plan for --------------redacted, b(2)----------------------- consisted of re-typing the contingency plan procedures in the test report and the system owner informing the individual performing the test that the system does not have an alternate manual process. The tabletop discussion held did not include a scenario or simulated incident to walk through how the system owner should react in certain situations. In addition, key participants[15] were not included in the tabletop discussion and roles, responsibilities and actions to be taken were not discussed.

The tests performed were limited because, according to NH officials, ensuring employees know what to do if the systems they use are not available would be a business continuity function and not a contingency plan function. Therefore, NH officials believed testing the viability of the contingency plan was outside of NH's responsibility. Specifically, one NH official stated the information system is a utility to assist employees in performing their jobs and it is not NH's responsibility if the system owner is unable to

[14] The contingency plan for -------------redacted, b(2)-------------- had not been tested at the time of our review.

[15] Key participants identified in the contingency plans include a Contingency Plan Director, Contingency Plan Manager, Damage Assessment Team, and Contingency Plan Recovery Team.

perform their mission without that system because that would be a continuity of operations plan function. A contingency plan differs from a continuity of operations plan because it provides the recovery and resumption procedures for an IT system, including procedures for recovering a system resulting from minor disruptions that do not necessarily require relocation to an alternate site.

NIST SP 800-34 further states plan testing is a critical element of a viable contingency capability because testing enables plan deficiencies to be identified and addressed. Testing also helps evaluate the ability of recovery staff to implement the plan quickly and effectively. Each IT contingency plan element should be tested to confirm the accuracy of the individual recovery procedures and the overall effectiveness of the plan. By not testing the contingency plans, NARA has no assurance the plans will actually work and may severely impact NARA's ability to recover its IT systems in the event of a disaster.

Recommendation 17: The Assistant Archivist for Information Services, along with the system owners, should develop tests of the system contingency plans to evaluate the viability of the plan procedures and determine the ability of recovery staff to implement the recovery strategy identified.

Management Comment(s)

The Assistant Archivist for Information Services concurred with the recommendation.

PROGRAM-LEVEL PLAN OF ACTION AND MILESTONES PROCESS

The program-level POA&M did not include all IT security weaknesses and vulnerabilities known to management. This occurred because NH officials did not establish a formal process to manage, prioritize, and track IT security weaknesses identified in the NARA Information Security Program. FISMA requires that federal agencies develop a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency. Without a complete POA&M, the CIO may not have proper visibility of IT security weaknesses and can not use the POA&M as an effective management tool to request and allocate resources for correcting IT security weaknesses.

FISMA requires that federal agencies develop a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency. OMB Memoranda 02-01 and 04-25 provided instructions on how to implement a POA&M process and the information needed to report and track weaknesses identified. The purpose of the POA&M is to help agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems.

According to NH officials, the program-level POA&M consisted of a Status of Audits and Evaluations spreadsheet maintained by NH and an Audit Action Summary database maintained by NARA Policy and Planning Staff (NPOL). However, these tracking mechanisms related to open audit recommendations and did not focus on IT security weaknesses. In addition, the spreadsheet and database did not include all the information required by OMB such as prioritization of the weaknesses, funding needed to correct the weakness, or the severity of the weakness.

In addition to audits, IT security weaknesses can be identified through internal reviews done by or on behalf of the agency such as annual security control testing and the C&A process. C&A testing conducted for NARA systems in FY 2007 identified systemic weaknesses within the NARA IT Security Program. However, an NH official stated he was unsure where to report these weaknesses because he did not want to include the same weakness on each system POA&M. Instead, the NH official included the weaknesses on the POA&M for the NARANet system. However, reporting the weaknesses on the NARANet system POA&M removed the CIO's visibility of the weaknesses because the CIO did not review system-level POA&Ms.

In addition to the systemic weaknesses, NH officials did not include all weaknesses identified during the 2nd quarter 2007 vulnerability scan. According to NH officials, all of the vulnerabilities had been corrected; however, we found 84 Remedy tickets related to the 2nd quarter 2007 vulnerability scan that had not been addressed.

Based on interviews with NH and NPOL officials, there appeared to be a disconnect between the POA&M process required by OMB and what NARA officials believed the POA&M process should be. NH officials believed all pertinent information was already included in the Status of Audits and Evaluations spreadsheet, therefore, they did not want to "create another document with no purpose."

During the audit, NH officials revised their Status of Audits and Evaluations spreadsheet with the intent of meeting the minimum OMB requirement for a program-level POA&M. Our review of the revised POA&M revealed that NH officials changed the format of the POA&M but continued to omit IT security weaknesses known to management.

The Exhibit 300 "Capital Asset Plan and Business Case" for the NARA IT Infrastructure included an IT security investment request of $9.8 million for FY 2007 to maintain and improve the level of IT security. The CIO's centralized security budget covered the expenses for centralized monitoring and response, enterprise-wide security infrastructure (e.g. firewalls), training and awareness, and certification and accreditation activities. This funding for IT security was provided without ensuring NH was making significant progress in overcoming security weaknesses. By not utilizing the POA&M as a tool to assist the CIO in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems, the CIO may not be appropriately allocating funding.

Recommendation 18. The Assistant Archivist for Information Services should develop a plan of action and milestone process that provides visibility over all IT security weaknesses and issue written procedures regarding that process.

Management Comment(s)

The Assistant Archivist for Information Services concurred with the recommendation.

SECURITY AWARENESS TRAINING FOR INDIVIDUALS WITH SIGNIFICANT SECURITY RESPONSIBILITIES

Only 35 of the 67 (52%) individuals with significant security responsibilities[16] completed the NARA Managers and Information System Security Officer (ISSO) training course and IT contractors were not required to complete the training even though they have significant security responsibilities. The purpose of this additional security awareness training was to provide current information about changes in IT security doctrine and reference policy and guidance affecting IT security programs. This occurred because NH officials did not have a process to track which individuals at NARA had significant security responsibilities and believed contractors met the training requirement based on job descriptions in the contracts. FISMA requires agencies to provide training to employees and contractors to inform them of the risks associated with their activities and their responsibilities in complying with agency policies and procedures designed to reduce these risks. If employees do not receive training at a level associated with their responsibilities, NARA risks security breaches resulting from employees who are not fully aware of their security roles and responsibilities.

NARA Notice 2007-177 "Mandatory IT Security Training," May 21, 2007, stated there were three types of training to select depending on your position and role within the organization. The notice required product owners, IT managers, and security professionals to take the "NARA Managers and Information System Security Officer" training course. According to an NH official, there was no clear definition of who constituted "people with significant security responsibilities" therefore, the NH official considered only ISSOs (approximately14 employees) to need the additional training. Further, the NH official stated NARA Notice 2007-177 was based on the notice from a previous year and should not have included the requirement for NARA managers to take the training in FY 2007.

NH officials did not require IT contractors to complete the training even though the contractors have significant security responsibilities over NARA IT assets and are IT security professionals. For example, IT contractors at NARA have access to NARA servers and provide access to NARA systems. Therefore, these contractors have significant security responsibilities at NARA and should have been required to take the additional training.

According to the documentation provided by NH officials, over 250 individuals completed the "NARA Managers and Information System Security Officer" training course. However, NH officials identified only 67 individuals as required to take the training. An NH official stated the list was comprised of current system owners, IT managers, and IT security professionals, but that the course was not targeted towards contractors.

OMB Memorandum 07-19 contained questions and answers to assist agencies in answering the FISMA reporting questions. One question asked "Is it the agency's

[16] The list of significant security personnel was provided by NH.

responsibility to ensure contractors have security training if they are hired to perform IT security functions? Wouldn't they already be trained by their companies to perform this work?" OMB responded "The agency should include in its contract the requirements for level of skill and experience. However, contractors must be trained on agency-specific policies and procedures, including rules of behavior." The CISO used this response to explain why NH contractors were not required to take the additional training course. According to the CISO, NH contractors satisfy the training requirement because their job descriptions prescribe the skills and experience needed to perform the job and the basic awareness course provided the agency-specific awareness and rules of behavior.

The purpose of the "NARA Managers and ISSOs" training course was to provide NARA IT system owners and managers, program and project managers, and persons providing IT security services with a source of current, up to date information about changes in IT security doctrine and reference links to policy and guidance affecting IT security programs. According to the training course introduction, this course was particularly targeted for those individuals whose jobs involve significant security responsibilities, associated with the management or technical oversight of NARA IT systems. Therefore, this course should have been required for all NARA employees with significant security responsibilities, including contractor employees.

Recommendation 19. The Assistant Archivist of Information Services should develop a process to identify employees with significant security responsibilities.

Management Comment(s)

The Assistant Archivist for Information Services concurred with the recommendation.

Recommendation 20. The Assistant Archivist for Information Services should require all individuals with significant security responsibilities, including contractor employees, to complete training based on the risk provided by their activities and develop a process to monitor compliance.

Management Comment(s)

The Assistant Archivist for Information Services concurred with the recommendation.

PRIVACY PROGRAM

Privacy Impact Assessments (PIAs) did not include information related to how personally identifiable information (PII) in the system would be secured and did not identify what choices were made as a result of performing the PIA. This occurred because the PIA template used did not contain a section for this information and Privacy officials were not aware these statements were required. OMB directed agencies to conduct PIAs and provided specific instructions on the information to be included. Without this information, the public, whose information may be stored in the system, does not have assurance their information is being properly protected.

We reviewed 10 PIAs and found the PIAs did not:

(a) affirm the agency is following IT security requirements and procedures;

(b) acknowledge the agency has conducted a risk assessment, identified security controls to protect the system, and implemented those controls;

(c) describe the monitoring, testing and evaluating to ensure controls continue to work properly and safeguard information;

(d) provide a point of contact for any additional questions from users; or

(e) identify what choices the agency made regarding an IT system or collection of information as a result of performing the PIA.

OMB Memorandum 03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 30, 2003, directs agencies to conduct reviews of how information about individuals is handled within their agency when they use IT to collect new information, or when agencies develop or buy new IT systems to handle collections of personally identifiable information. OMB's Implementation Guidance for Section 208 of the E-Government Act requires agencies to conduct a privacy impact assessment for electronic information systems and collections and, in general, make them publicly available. OMB 03-22 provides guidance on which systems require a PIA and the specific information that must be analyzed and described in the PIAs.

A PIA was available on the Archives website for those systems identified as containing PII, however, the template used for the PIAs did not directly match to the OMB 03-22 required contents. According to a privacy officer, the format chosen was a collaborative effort between NH and NARA General Counsel Officials. The Privacy Official believed all the required information was included and was not aware of the additional requirements. Privacy officials received clarification from OMB regarding the content required and agreed to revise the PIAs to include this additional information.

Recommendation 21. The Senior Agency Official for Privacy, in coordination with the Assistant Archivist for Information Services, should revise the existing Privacy Impact Assessments and the Privacy Impact Assessment template to incorporate information related to how Personally Identifiable Information in the system is secured and identify what choices were made as a result of performing the Privacy Impact Assessment.

Management Comment(s)

The Senior Agency Official for Privacy concurred with the recommendation.

APPENDIX A. IT SYSTEMS REVIEWED AND RESULTS OF THE REVIEW

System	Authorized to Operate?	Complete Security Plan?	Complete POA&M?	Updated Contingency Plan?	Adequate Contingency Plan Test?
--redacted, b(2)--	Yes	No	No	No	No
--redacted, b(2)--	Yes	Yes	No	No	No
--redacted, b(2)--	Yes	No	No	No	No
--redacted, b(2)--	No	No	Yes	No	No
--redacted, b(2)--	Yes	No	No	No	No
--redacted, b(2)--	Yes	No	Yes	No	No
--redacted, b(2)--	Yes	No	No	No	No
--redacted, b(2)--	Yes	No	Yes	No	No
--redacted, b(2)--	Yes	No	No	No	N/A
--redacted, b(2)--	Yes	No	No	No	No
--redacted, b(2)--	Yes	No	Yes	Yes	Yes
--redacted, b(2)--	Yes	No	No	No	No

National Archives and Records Administration

*8601 Adelphi Road
College Park, Maryland 20740-6001*

Date: March 17, 2008

To: Paul Brachfield (OIG)

From: Martha Morphy (NH)

Subject: Comments on the OIG Audit Report No. 08-05: Audit of NARA's Compliance with the Federal Information Security Management Act for FY 2007

We are in receipt of your report and would like to thank you for the opportunity to respond to its findings and recommendations. We would particularly like to express our appreciation for the hard work done by your staff and auditors in the preparation of the report, the effort has yielded a product which is informative and which will be of significant value to our security program.

We concur with all of the recommendations in the report, and will provide a summary response here, with details in the audit action plan. Otherwise, the findings of the report provide a detailed view of problems which are the subject of more general efforts associated with our plan to remove the external material weakness that was declared in the FY 2007 PAR, and where steps have been taken to address these problems, they will be detailed in our audit action plan.

General Response to Recommendation 1.

high b(2)

Recommendation 1: Concur

General Response to Recommendations 2-10

The report notes that while a number of incidents recorded by NARA's IDS systems were not reported to US CERT within specified timeframes, these incidents were all resolved internally and on the basis of standard operating procedures which did not require the convening of the NARA CIRT. We believe that these discrepancies can be addressed. Efforts to revise and perfect the Incident Response Policy and the guidance in the Handbook are ongoing, and will be described in the Audit Action Plan.

Recommendation 2: Concur
Recommendation 3: Concur
Recommendation 4: Concur
Recommendation 5: Concur
Recommendation 6: Concur

Recommendation 7: Concur
Recommendation 8: Concur
Recommendation 9: Concur
Recommendation 10: Concur

General Response to Recommendations 11-13.

Efforts to address process and documentation limitations of the current Certification and Accreditation packages are ongoing as part of the response to the Material Weakness. Specific initiatives which address the recommendations in this section will be detailed in the audit action plan.

Recommendation 11: Concur
Recommendation 12: Concur
Recommendation 13: Concur

General Response to Recommendation 14.

In 2006 NARA issued updated versions of NARA Directive 202 and Directive 804 which clearly established the roles and responsibilities necessary to comply with this recommendation.

At that time NAS and NHI began a review of the certification status of the SCI systems. That review determined that NARA had consistently and properly certified the SCI systems on a regular basis, but had not been able to maintain contact with the accrediting agency which sponsors those systems for the DNI. Resource constraints in the office of the DNI are a reality, and despite efforts to secure accreditation decisions, there are currently three SCI systems which have been tested and recommended for certification, but which have no accreditation decision.

The DAA will be meeting with NARA program officials to establish actionable dates for the certification of these systems, and those details will be provided in the audit action plan..

Recommendation 14: Concur

General Response to Recommendations 15-20.

We concur with the findings and the recommendations. Actions being taken in response to the material weakness and the reportable condition will be reviewed to assure that the specifics of these findings are addressed by those initiatives.

Recommendation 15: Concur

Recommendation 16: Concur
Recommendation 17: Concur
Recommendation 18: Concur
Recommendation 19: Concur
Recommendation 20: Concur

General Response to Recommendation 21.

This will be addressed by the Privacy Officer.

Please call —— b(6) —— at 301-837-—— for any questions regarding this response.

Martha Morphy

MARTHA MORPHY
Assistant Archivist for Information Services

National Archives and Records Administration

8601 Adelphi Road
College Park, Maryland 20740-6001

Date: March 18, 2008

To: James Springs, OIG

From: Gary M. Stern, NGC

Subject: OIG FISMA Audit Report

The Office of General Counsel (NGC) concurs with privacy related recommendation 21, found in the Office of Inspector General's FISMA Audit Recommendations.

Any questions related to this memo can be addressed to Ramona Oliver, NARA Privacy Act Officer.

GARY M. STERN
General Counsel/
Senior Agency Official for Privacy