Audit of NARA's Classified Systems

OIG Audit Report No. 12-15

July 23, 2012

Table of Contents

Executive Summary

The National Archives and Records Administration (NARA) Office of Inspector General (OIG) completed an audit of the classified information systems at NARA. In accordance with Federal requirements, NARA has developed policy to protect its classified systems. NARA Directive 202 establishes the agency's Classified Information Security Program. Further, NARA Directive 804 establishes requirements for the operation, management, and control of information systems. During this audit, we assessed whether NARA's classified information systems were properly managed and adequately secured.

Executive Order 13526, *Classified National Security Information*, dated December 29, 2009, directs the agency head or senior agency official to establish uniform procedures to ensure the confidentiality, integrity, and availability of automated information systems. This includes networks and telecommunications systems, that collect, create, communicate, compute, disseminate, process, or store classified information.

Our audit found that the confidentiality and security of classified information is at risk. Although NARA has developed classified information system policies in accordance with Federal guidelines, the Office of Information Services personnel, system owners, and designees responsible for ensuring the confidentiality, integrity, and availability of NARA classified information systems have not consistently implemented these requirements. Specifically, of the seven classified systems reviewed, only one has a current authorization to operate. Further, NARA officials have not taken the appropriate and sufficient steps to adequately manage their classified systems. Management deficiencies identified include:

- Weaknesses recognized during annual security assessments were not always communicated and properly addressed;
- Plans of Actions and Milestones were not always maintained, updated, or reviewed, as required;
- Inventories of systems and components were not always updated and completed;
- Contingency Plans had not been developed and tested for all classified systems; and
- Continuous monitoring strategies had not been established or implemented.

As a result, the classified information NARA is entrusted with overseeing and securing is not afforded the magnitude of protection required, placing undue risk on the overall security of information at the highest classification levels. Without the proper oversight and accountability to ensure implementation of NARA's Classified Information Security Program as it relates to classified information systems, NARA is hindered in its ability to adequately identify and reduce the vulnerabilities and control failures associated with its classified systems, which places the confidentiality and security of classified information at risk. Although all risks cannot be avoided, the controls and processes identified in this report are fundamental to the security of NARA's classified information systems.

Due to security considerations, specific information regarding the locations and systems reviewed have been omitted from this report and supplied to NARA officials separately. This report contains 8 recommendations to assist the agency in strengthening the security and control of its classified information systems.

Background

As the Nation's record keeper, NARA receives classified records in electronic and paper formats, which are then processed and stored on various NARA classified systems. These classified systems have specialized security needs and must be protected at a higher level than unclassified systems in order to guard against unauthorized disclosure as well as loss or modification. It is critical that NARA ensure the appropriate security controls are applied to its classified systems or the safety of these systems and the information contained on these systems are at risk. Recent events surrounding the disclosure of U.S. Government documents by WikiLeaks have emphasized the need to protect and secure our classified national security information systems.

In 2004, we conducted a similar audit of NARA's classified Information Technology (IT) systems[1]. In this previous audit, we found NARA had not developed or implemented a classified IT systems security program that included updated guidance pertaining to the technical security of classified systems. NARA had also not created a complete classified computer systems inventory listing. Consequently, numerous security weaknesses were found in the classified system reviewed. Therefore, we recommended the Archivist ensure that NARA classified systems were centrally managed by technically qualified personnel by redesignating responsibility for those systems. We also recommended the development of the NARA Classified IT Systems Security Program; the identification and inventory of all NARA classified systems; and an initial certification and accreditation (C&A) of these systems be completed. Management concurred and completed each of these recommendations.

All NARA IT systems processing or storing classified information must be designed and operated in a manner to protect the availability, integrity, and confidentiality of the information. NARA Directive 202 provides the necessary guidance for the protection of classified information before it is entered into an IT system, classified output that has been generated from the system, and for the physical environment surrounding the system. Further, NARA Directive 202 establishes the NARA Classified Information Security Program and identifies the responsibilities of NARA officials and designated personnel for the protection and control of classified national security information, regardless of the media. Additional policies related to the operation, management or control of information systems are contained in NARA Directive 804, *Information Technology Systems Security*, and other Federal standards and directives, including the Director of Central Intelligence Directive (DCID) 6/3, *Protecting Sensitive Compartmented Information within Information Systems* for Sensitive Compartmented Information (SCI) level systems.

[1] NARA OIG Report No. 04-10, "Assessment of the Controls and Security of NARA Classified Systems," March 31, 2004

Objectives, Scope, Methodology

The overall objective of this audit was to determine whether NARA's classified systems were properly managed and adequately secured. Specifically, we sought to determine whether the security of NARA's classified systems complied with Federal and NARA security policies and guidelines.

To accomplish our objective, we reviewed NARA policies governing classified information and systems and examined the security of seven classified systems at NARA. We interviewed IT Security personnel, system owners, and system and security personnel. Further, we obtained available classified system security documentation. We compared the implementation of NARA's Classified Information Security Program (as it relates to Information Systems) to NARA policy and Federal requirements, specifically: the Federal Information Security Management Act of 2002, (Public Law 107-347 Sec. 301); Executive Order 13526, *Classified National Security Information*; National Institute of Standards and Technology (NIST) SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*; NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*; NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System*; and Director of Central Intelligence 6/3, *Protecting Sensitive Compartmented Information within Information Systems*.

Our audit work was performed at Archives I and Archives II between February 2011 and June 2012 (however, audit work was postponed at times due to limited staffing resources). We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Audit Results

1. Implementation of Risk Management Framework on NARA's Classified Information Systems

Although NARA has developed classified information system policies in accordance with Federal guidelines, the Office of Information Services personnel, system owners, and designees responsible for ensuring the confidentiality, integrity, and availability of NARA classified systems have not consistently implemented these requirements. Specifically, this is apparent in the classified systems risk management process. Of the seven systems reviewed, only one has a current authorization to operate. This condition exists because required coordination efforts between Information Security personnel, system owners, and authorizing officials were not conducted and authorization packages were not appropriately completed or updated. As a result, NARA lacks assurance its classified data and systems are secure from numerous threats and vulnerabilities.

NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, includes guidelines for conducting the activities of security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring. Further, NIST SP 800-37 identifies three key documents used in support of the risk management process, these include: 1) security plans; 2) security assessment reports; and 3) plans of actions and milestones. These documents are used by authorizing officials to make risk-based decisions in the security authorization process for their information systems.

NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, provides additional guidance on risk management through the implementation of security controls. These guidelines apply to all components of information systems that process, store, or transmit Federal information, including classified systems. NIST SP 800-53 states secure information systems require well-defined security requirements and security specifications, as well as comprehensive system security planning and life cycle management. These guidelines identify the security plan as an important component of the process. NIST SP 800-53 defines the security plan as the formal document providing an overview of the security requirements for an information system, which describes the security controls in place or planned for meeting those requirements.

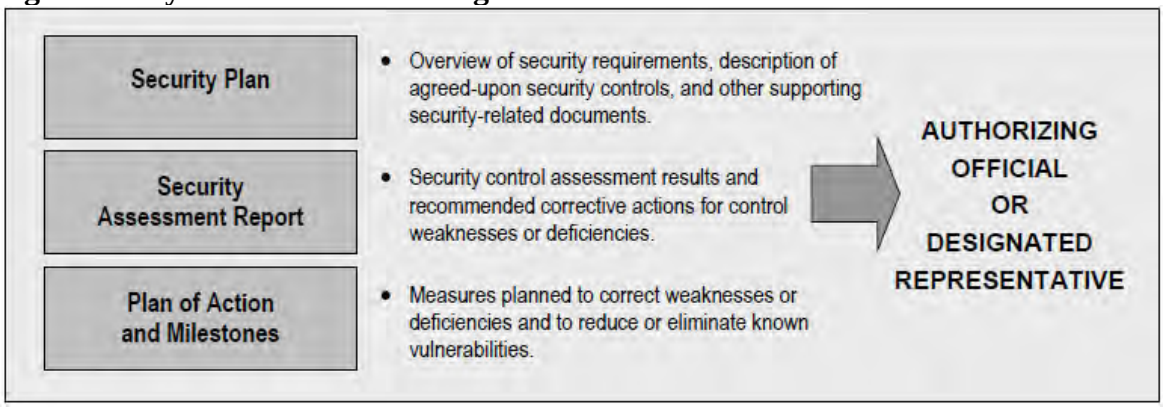
NARA policy incorporates many of the NIST guidelines related to the risk management of classified systems. Specifically, *NARA IT Security Requirements*, within the scope of this audit, establishes requirements related to the security planning, risk assessment, and

security authorization. These requirements include the development and update of system security plans, security assessment reports, and plans of actions and milestones. Further, NARA policy requires the Office of Information Services to ensure information systems are authorized to operate and the security authorizations are updated at least annually.

Classified System Authorization Documentation

NARA has outlined procedures to meet the Authorization requirements of the Risk Management Framework. Specifically, *NARA IT Security Methodology for C&A and Security Assessment* describes the documentation and assessment results used by NARA's authorizing officials. These documents and reports, which are included in the system authorization packages, provide essential information needed to make risk-based decisions on whether to authorize operation of information systems or designated sets of controls. The chart below provides an overview of the authorization package documents.

Figure 1. Key Authorization Package Documents



Security Plan. According to NARA's C&A Methodology, the security plan is prepared by the information system owner. The security plan provides an overview of the security requirements and describes the security controls in place or plans for meeting those requirements. The security plan also contains information related to risk assessments, contingency planning, and the continuous monitoring strategy. *NARA IT Security Requirements* stipulate classified system security plans must be reviewed and updated at least annually.

The Office of IT Security provided security plans for each of the seven classified systems reviewed during this audit. However, none had been updated within the last year in accordance with NARA requirements. Most of the security plans reviewed had last been approved over four years ago with no further indication of updates or revisions. Further, a majority of the classified system security plans reviewed listed retired NARA personnel in key security roles for the systems. In addition, a number of the security plans

identified important security controls that required strengthening. However, there is no evidence such activities took place. The deficiencies identified relate to setting audit log files to read only access, developing off-site backup storage requirements, auditing system-level actions, and establishing appropriate access password controls.

Security Assessment Report. NARA's C&A Methodology indicates the security assessment report is prepared by the security control assessor. The security assessment report provides the results of assessing the implementation of the security controls identified in the security plan to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the specified security requirements. NARA's C&A Methodology states the security assessment report is to be updated on an ongoing basis whenever changes are made to the security controls employed within or inherited by the information system.

Further, *NARA IT Security Requirements* state IT Security staff shall assess the security controls in the information system at least annually. Updates to the security assessment report help ensure the information system owner, common control provider, and authorizing officials maintain the appropriate awareness with regard to security control effectiveness. In addition, NARA policy requires security assessment reports to contain a list of recommended corrective actions for any weaknesses or deficiencies identified in the security controls.

The Office of IT Security provided security assessment reports for each of the classified systems reviewed. All seven of the assessment reports were completed in September 2010. Updates were requested, however, IT Security personnel indicated the September 2010 security assessment reports were the most recent. Although seven assessment reports were provided, one of the classified systems reviewed has four different instances, each located at a different facility across the country. Despite the unique security concerns of each location, only one security assessment was conducted for all four instances, focusing on only one location. Further, the security assessment reports for the seven classified systems identified a combined total of over 315 failures. A number of these control failures were identified across all classified systems reviewed, these systemic control failures involve:

- Response to Audit Processing Failures,
- Baseline Configuration,
- Configuration Settings,
- Least Functionality,
- Vulnerability Scanning, and
- Malicious Code Protection.

Further, 54 particular controls failed in three or more of the seven classified systems reviewed. Despite these failures, recommended corrective actions were not typically documented in the security assessment reports, as required. In addition, many of the documents used in support of the security assessments—such as the system security plans mentioned previously—have not been updated in the past three or four years, which further degrades the accuracy of the assessments.

Plan of Action and Milestones (POA&M). NARA's C&A Methodology assigns the responsibility of preparing the POA&M to the system owner or common control provider. The POA&Ms describe specific measures planned to correct weaknesses or deficiencies in security controls identified during the security assessment and to address known vulnerabilities in the information system. *NARA IT Security Requirements* state the system owner shall update existing POA&Ms not less than annually based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

The Office of IT Security provided POA&Ms for six of the seven classified systems reviewed. Although each of the systems underwent a security assessment in September 2010, none of the POA&Ms were updated to reflect the more recent weaknesses identified. Further, the POA&Ms provided listed nearly 90 weaknesses that are still classified as "ongoing," some of which date back to 2006. Examples of these ongoing weaknesses include:

- Antivirus software/application not installed/updated;
- Need for Sensitive Compartmented Information Facility (SCIF) accreditation renewal;
- Inadequate labeling of hardware to reflect appropriate classification level;
- SCIF is not in accordance with Director of Central Intelligence Directive (DCID);
- Insecure/not properly retained audit logs;
- Inadequate review of audit logs;
- Uncleared personnel allowed to perform maintenance on classified system without being recorded on the maintenance log;
- Co-location of classified workstations with lower classified systems;
- System Security Plans not updated to reflect actual processes or state of system;
- Lack of data sanitizing procedures;
- Duties and responsibilities of the System Administrator had not been developed in accordance with DCID 6/3;
- Adequate password policies not implemented;
- Lack of configuration management policies; and
- Inadequate backup process.

Many of the POA&Ms reviewed state "keeping the documentation current is a simple process and is well worth the minimal effort and cost in the long-run." However, this "minimal effort" to reduce the risk of NARA's classified systems is not consistently performed. Further, a number of the weaknesses documented in the POA&Ms (and listed above) remain as control failures in the most recent Security Assessments. When asked why the documentation had not been updated or tracked, the Office of Information Services indicated it is difficult to obtain required documentation from system owners and despite establishing cutoff dates, system owners "file away the POA&Ms and do nothing with them."

Continuous Monitoring

As mentioned previously, according to NARA's C&A Methodology, system security plans document the continuous monitoring strategy for each system. Further, *NARA IT Security Requirements* state for all data, the IT Security Staff must establish a continuous monitoring strategy and implement a continuous monitoring program. This includes ongoing security control assessments, annual reporting of the security state of the information system, and for data deemed by the NARA system owner to require additional integrity protection, NARA IT Security staff shall plan, schedule, and conduct security assessments to ensure compliance with all vulnerability mitigation procedures.

Despite the requirements to include a continuous monitoring strategy within the classified system security plan, none of the systems reviewed contained such information. Most of the classified system security plans do not mention continuous monitoring, or generally state "detection and/or monitoring tools are not required because [the classified system] is a self-contained system with no external connectivity." However, according to NIST guidance, automated support tools are only one component of continuous monitoring. The process also includes—among other monitoring activities—assessing the security impacts on an information system resulting from planned and unplanned changes to the hardware, software, firmware, or environment of operation—using people, processes, and technologies.

NARA IT Security personnel stated most of NARA's continuous monitoring processes are being developed to work over the network, therefore, the classified systems—which are standalone—will not benefit. IT Security personnel stated they are still struggling with continuous monitoring of the unclassified systems, let alone classified systems. However, NARA's C&A Methodology states failure to maintain an effective continuous monitoring program may be grounds for rescinding an authorization decision. Without current classified system security information made available through continuous monitoring, authorizing officials are limited in their ability to make risk-based decisions.

Authorization Status of NARA's Classified Information Systems

The documentation used to support management's risk assessments of classified systems is incomplete, outdated, and inconsistent. The three key documents approving authorities use in their assessments of the classified systems: System Security Plans, Security Assessment Reports, and Plans of Actions and Milestones do not reflect the level of detail or current information needed to justify approval. As a result, of the seven systems reviewed, only one has been certified and authorized to operate. According to IT Security personnel—for certain high confidentiality systems—NARA has had difficulty in getting authorization feedback from the Central Intelligence Agency, which has impaired the timely authorization of these systems. However, this does not account for the incomplete and outdated authorization packages NARA is using. Complete and acceptable packages should have been assembled, compiled, and submitted by the system owner prior to the authorization decision.

NARA IT Requirements state that for all data, the NARA Office of Information Services shall ensure the authorizing official authorizes the information system for processing before commencing operations. DCID 6/3, *Protecting Sensitive Compartmented Information within Information Systems*, provides similar authorization to operate requirements for SCI systems. DCID 6/3 states if the designated approving authority neither accredits the system, nor grants an interim approval to operate, then the requestor must modify the system or its safeguards, and repeat the accreditation process until the system is accredited, granted interim approval to operate, or disallowed to operate. Despite these requirements, NARA classified systems continue to operate without current authorizations. When asked if any of the classified systems were shut down, Office of IT Security personnel stated NARA does not shut down systems, even if they do not have an authorization to operate. This stance by the Office of IT Security weakens NARA's Classified Information Security Program by allowing systems to run without ensuring compliance with all confidentiality and vulnerability mitigation procedures.

Implications of Inadequate Risk Management Framework Implementation

NARA has established policy to protect classified systems from the elevated risks associated with such systems, yet classified systems continue to operate without meeting the security requirements established to ensure confidentiality, integrity, and availability. As a result—in the current environment in which agencies are on heightened alert over recent classified system breaches—NARA lacks assurance its classified data and systems are secure and controls are in place and effective in protecting classified data against threats and vulnerabilities.

Recommendations

We recommend the Executive for Information Services/Chief Information Officer (I), in coordination with the Chief Operating Officer (C):

1. Ensure all classified system authorization packages are updated in accordance with NARA policy;
2. Establish a timeline for review and approval of authorization documents;
3. Develop a continuous monitoring strategy for classified systems requiring system owners on at least a quarterly basis to assess security controls and inform authorizing officials when changes occur that may impact the security of the system; and
4. Obtain authorizations to operate for each of the classified systems or disallow them in accordance with NARA and Federal policy.

Management Response

Management concurred with the recommendations.

2. Oversight and Security Control of NARA's Classified Information Security Program

NARA IT officials and designated personnel at all levels are not meeting their responsibilities in the oversight, protection, and control of classified information systems in accordance with NARA's Classified Information Security Program. This is due to a general lack of accountability and coordination by the Office of Information Services, system owners, and security and system personnel—specifically in terms of accomplishing classified information system security requirements. As a result, NARA is hindered in its ability to adequately identify and reduce the vulnerabilities and control failures associated with its classified systems, which places the confidentiality and security of classified information at risk.

The *Federal Information Security Management Act of 2002* (FISMA) requires each agency to develop, document, and implement an agencywide information security program. The program is to provide information security for the information and information systems supporting the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. Further, FISMA requires the information security program to include periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency, including classified systems.

Within the scope of classified information systems and security, NARA has issued two primary Directives. The first of these, NARA Directive 202, *NARA Classified Information Security Program*, establishes NARA's Classified Information Security Program and identifies the responsibilities of NARA officials and designated personnel in the protection and control of classified national security information. In addition, NARA Directive 202 is supplemented by the *NARA Classified Information Security Program Handbook*. The purpose of the handbook is to serve as a "how to" guide for the NARA Information Security Officer and Information Security Program Managers to use in promoting a viable and dynamic classified information security program.

The second Directive, NARA 804, *Information Technology Systems Security*, establishes policy and guidance for securing all electronic information collected or maintained by or on behalf of NARA, and the electronic information systems used or operated by or on behalf of NARA. NARA 804 defines the role of IT security in the context of an overall enterprise architecture. In addition, the Directive delineates the security management program structure, assigns responsibilities, and creates a foundation to manage progress and compliance.

Classified Information Security Program Responsibilities

NARA's policy outlines Classified Information Security Program roles and responsibilities starting at the head of the agency and ending at the final user of the information. The Archivist is responsible for committing senior management and resources to the successful implementation of the program. Other key roles—within the scope of this audit—include the Chief Information Officer, Chief Information Security Officer, IT Security Staff, System Owner, Information System Security Officer, and Information Security Program Manager. The responsibilities of these roles as they relate to classified information system security are outlined below:

Chief Information Officer (CIO). The CIO ensures development and implementation of the NARA IT Security program and NARA IT security architecture conform to all NARA and other Federal standards, policies, and guidelines. The CIO is the designated authorizing official for agency-wide general support systems and is the co-authorizing official with other senior officials for selected agency information systems. The CIO designates the senior agency information security officer.

Chief Information Security Officer (CISO). The CISO is the senior agency information security officer responsible for the implementation of NARA 804 and its policies. The CISO directs the NARA IT Security Program with the mission and resources to assist in ensuring agency compliance with FISMA. Further, the CISO is the agency official responsible for carrying out the chief information officer responsibilities under FISMA.

IT Security Staff. The IT Security staff plans and manages the IT Security program in conformance with the IT Security Architecture. The staff assists in the development of the security architecture, assures the appropriate integration of security controls as part of the systems engineering process, and provides guidance and assistance to systems owners on matters of IT security.

System Owner. The system owner is the official responsible for the procurement, development, and operation and maintenance of the system. Further, the system owner is responsible for developing and submitting the authorization package. System owners also evaluate the cost and benefits of system features, including the security costs of mitigating vulnerabilities associated with the system. In addition, system owners identify or designate responsibility for the Information Systems Security Officer.

Information Systems Security Officer (ISSO). The ISSO has the responsibility to ensure the appropriate operational security posture is maintained for an IT system or program. The ISSO assists in determining the security controls appropriate for the system, and provides information necessary to complete regular assessments of the system and the POA&M, which tracks response to internal and external audit findings.

Information Security Program Manager (ISPM). The ISPM develops standard operating procedures addressing information security requirements specific to the activity for which they are responsible. In addition, the ISPM assists the ISSO, in coordination with the system owner, as necessary to develop SSPs, risk assessments, contingency plans, obtain certification and accreditation of all classified computer systems, and report computer-related security incidents for all computer systems under the control of their activity.

Based on the roles listed above, NARA has developed multiple levels of oversight in its governance of the security and management of classified information systems. However, despite these oversight and management roles, a number of Classified Information Security Program objectives and requirements remain unmet. The following section describes some of the management and implementation deficiencies identified in NARA's Classified Information Security Program as it relates to classified information systems.

Implementation of NARA's Classified Information Security Program

A basic requirement in implementing a Classified Information Security Program involves establishing and maintaining a current inventory of classified systems. However, during our tours of the Sensitive Compartmented Information Facilities (SCIFs) and a review of NARA's 2011 Performance and Accountability Report, we identified additional classified systems not reflected in the inventory list provided by the Office of Information Services. Further, a number of the systems included in the inventory were considered to be inactive or decommissioned. An OIG audit conducted in 2004 identified similar inadequacies pertaining to NARA's classified system inventory[2].

Further, NARA policy establishes requirements pertaining to information system component inventory. *NARA IT Security Requirements* state for all data, the system owner shall develop, document, and maintain an inventory of information system components that accurately reflects the current information system. In addition, for data requiring greater integrity, the system owner shall verify all components within the authorization boundary of the information system are either inventoried as a part of the system or recognized by another system as a component within that system. During our tour of classified facilities, we noted items within the classified system boundaries that were not included in the component inventory list. These items included printers, toggle switches, and a smart uninterruptible power supply backup.

[2] NARA OIG Report No. 04-10, "Assessment of the Controls and Security of NARA Classified Systems," March 31, 2004

Another component of the Classified Information Security Program involves obtaining authorization for the classified systems to operate (see Finding 1). NARA policy states it is the responsibility of the system owner to assemble, compile, and submit the authorization package. In addition, as noted above, it is also the responsibility of the IT Security staff, ISSO, and ISPM to aid the system owner in this process. Therefore, in order for the authorization to take place, each classified system must have an appointed system owner who works in coordination with IT Security staff and designated system and security personnel.

The Office of IT Security provided the most recent system owner appointment letters for the classified systems reviewed. Most of the letters were last signed in mid-2009. At least one these appointed system owners no longer works at NARA. Two other system owners listed on appointment letters do not match those named in more recent system documentation. Further, one person who was appointed system owner to four classified systems had relinquished these duties as a result of NARA's reorganization. At the time of this audit, new system owners had not been appointed.

Due to the important role system owners play in the security of classified systems, it is vital that the appointments remain accurate and the system owners acknowledge their responsibilities. Up-to-date appointment letters facilitate this acknowledgement by requiring the system owners to sign and date the letter which outlines their responsibilities. Some of the acknowledged responsibilities listed on the appointment letters provided include:

- Ensuring security requirements for the system will be met;
- Assigning, in writing, an ISSO;
- Informing the Office of IT Security of the need to conduct a certification and accreditation of the system; and
- Ensuring adequate resources are available for the certification and accreditation effort.

Despite these acknowledged requirements, six out of the seven System Security Plans—which are required to provide overviews of the security requirements and security controls in place for each of the systems—have not been updated in over three years. Additionally, of the seven systems reviewed, the Office of IT Security was only able to provide signed ISSO appointment letters for four systems. Further, only one of the seven classified systems had a current certification and accreditation.

In addition to the responsibilities listed above, the system owner appointment letters state the system owners may delegate day-to-day authority, as applicable, to an ISSO to

perform a number of security duties. Examples of these duties include:

- Providing and maintaining all documentation as required for the certification and accreditation process and retaining the results from the Office of IT Security;
- Taking appropriate steps to reduce or eliminate vulnerabilities;
- Ensuring the development and annual update of the system security plan;
- Deploying and operating the system according to the security requirements in the system security plan;
- Providing the continuous monitoring of the information system;
- Coordinating the development of a Contingency Plan and ensuring the plan is tested and maintained annually;
- Establishing system-level POA&Ms and implementing corrective actions to develop, implement, manage, and track these actions; and
- Working closely with the Office of IT Security and other IT managers to ensure a complete understanding of the risk.

Despite the listing of these duties on the system owner and ISSO appointment letters, most were not accomplished for the systems reviewed. For example, system personnel were unable to provide requested certification and accreditation documents. Further, efforts to address ongoing vulnerabilities have been lacking, some POA&Ms with identified deficiencies have not been updated in the past four years. Additionally, IT Security staff indicated continuous monitoring efforts of classified systems have been minimal.

The appointment letters also include duties involving contingency planning. *NARA IT Security Requirements* establishes system owners must develop contingency plans for all information systems. System owners are required to review the plans at least annually. Further, the contingency plans are required to be reviewed and approved by NARA Security staff.

IT Security personnel were able to provide updated contingency plans for five of the seven classified systems reviewed. However, none of the contingency plans showed evidence of NARA Security staff review or approval, as required. In addition, five of the seven Security Assessment Reports associated with these systems identified contingency planning failures. Further, a number of issues were identified in the contingency plans provided, some of which include:

- System owner designation that differs from appointment letter;
- Incomplete key personnel contact lists;

- Contingency plan responsibilities assigned to a position that is vacant or unidentified; and
- Incomplete records documenting changes to the contingency plan.

For classified systems requiring moderate or high availability, *NARA IT Security Requirements* stipulate the NARA system owner shall plan for the resumption of essential missions and business functions within 24 hours for classified information systems of contingency plan activation. Further, the NARA system owner shall plan for the full resumption of missions and business functions within 5 days of contingency plan activation. According to the system documentation provided, two of the seven systems reviewed required elevated levels of availability. However, of these two classified systems, neither had contingency plans or test plans reflecting this heightened availability level.

NARA IT Security Requirements state the system owner or ISSO shall test or exercise the contingency plan at least annually to determine the plan's effectiveness, as well as the system owner or ISSO's readiness to execute the plan. Further, for classified systems, system owners are required to conduct backups of user-level and system-level information contained in the information system at least weekly. IT Security Personnel were able to provide test plans for five of the seven classified systems reviewed. Despite the annual requirement, only four of the classified system contingency test plans were updated in the past year. Of those four, only one contained complete and detailed results. Further, Security Assessment Reports identified failures related to system backups in four of the seven classified systems reviewed.

Another duty listed on the appointment letters involves working closely with the Office of IT Security and other IT managers to ensure a complete understanding of the risk. This is further detailed in NARA 804, which identifies providing guidance and assistance to system owners as one of the roles of IT Security staff.

During our audit interviews, system owners, ISSOs, and designees were asked about system documentation efforts and status. Interviewees were often unaware of the status of the key oversight and security documents for their respective systems. Further, despite being responsible for maintaining certification and accreditation documents, the interviewees were often unable to provide copies. The IT Security staff responsible for assisting system owners stated most of the classified system owners do not have an IT background. As a result, IT Security staff indicated system owners face difficulties in meeting their more technical responsibilities.

Conversely, some system owners mentioned they did not always receive adequate feedback from the Office of IT Security during the authorization process. Examples included providing the Office of IT Security with updates to documents without ever

hearing back from them and not obtaining results of security assessments performed by the Office of IT Security. Further, discrepancies existed between systems owners and the Office of IT Security regarding responsibility for implementing corrective actions. The chart below (Figure 2) depicts the status of key system documents for the seven classified systems reviewed.

Figure 2. Status of Key System Documents

System	Authorized to Operate?	Updated Security Plan?	Complete POA&M?	Updated Contingency Plan?	Adequate Contingency Plan Test?
Classified System #1	**No**	**No**	**No**	**No**	**No**
Classified System #2	**No**	**No**	**No**	**Yes**	**No**
Classified System #3	**No**	**No**	**No**	**Yes**	**No**
Classified System #4	**No**	**No**	**No**	**Yes**	**No**
Classified System #5	**No**	**No**	**No**	**Yes**	**No**
Classified System #6	**Yes**	**No**	**No**	**Yes**	**Yes**
Classified System #7	**No**	**No**	**No**	**No**	**No**

NARA policy establishes roles and responsibilities to ensure IT Security Staff, systems owners, ISSOs, and ISPM assist one another in completing system security documentation used in the certification and accreditation, contingency planning, and security efforts of each classified system. The status of the documents listed above illustrates a need for greater accountability and coordination in the implementation of NARA's Classified Information Security Program as it relates to classified information systems. The Office of IT Security acknowledged the security documentation for classified systems were not kept up-to-date. Difficulty in obtaining documentation from system owners was cited as the main factor in the lack of current security documentation.

Implications of Inadequate Oversight and Security Control of Classified Systems

Although NARA policy establishes responsibility for the CIO and CISO to implement NARA's IT Security program and NARA Directive 804 requirements, numerous inadequacies identified in our review of NARA's classified information systems indicate this responsibility is not being fulfilled. Specifically, NARA classified systems are not appropriately authorized, system security documentation is not complete, and key system

and security personnel have not been appointed to support these efforts, as required. Without the proper oversight and accountability to ensure implementation of NARA's Classified Information Security Program as relates to classified information systems, NARA is hindered in its ability to adequately identify and reduce the vulnerabilities and control failures associated with its classified systems, which places the confidentiality and security of classified information at risk.

Recommendations

We recommend the Executive for Information Services/Chief Information Officer (I), in coordination with the Chief Operating Officer (C):

5. Re-evaluate responsibilities among IT Security staff, system owners, ISSOs, and ISPMs to ensure they match the required expertise within each role;
6. Ensure that IT officials, system owners, and system and security personnel are aware of their classified system oversight roles and responsibilities;
7. Maintain current documentation to support each system has an appointed system owner and ISSO; and
8. Ensure all contingency plans are updated, completed, reviewed, and tested in accordance with NARA policy.

Management Response

Management concurred with the recommendations.

Appendix A – Acronyms and Abbreviations

C&A	Certification and Accreditation
DCID	Director of Central Intelligence Directive
ISSO	Information System Security Officer
IT	Information Technology
NARA	National Archives and Records Administration
OIG	Office of Inspector General
POA&M	Plan of Actions and Milestones
SCI	Sensitive Compartmented Information
TS	Top Secret

Appendix B - Management's Response to the Report

NATIONAL ARCHIVES

Date: JUL 18 2012

To: Paul Brachfeld, Inspector General

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

Subject: OIG Revised Draft Audit 12-13, Audit of NARA's Classified Systems

Thank you for the opportunity to provide comments on this draft report. We concur with the eight recommendations in this audit, and will begin work on an action plan when the final report is issued. We have no other comments.

If you have any questions or need additional information on these comments, please contact Mary Drak by phone at 301-837-1668 or via email at mary.drak@nara.gov.

David S. Ferriero
Archivist of the United States

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

Appendix C - Report Distribution List

David S. Ferriero, Archivist of the United States (N)
Tom Mills, Chief Operating Officer (C)
Michael Wash, Executive for Information Services and Chief Information Officer (I)
Mary Drak, Performance and Accountability Staff (CP)