United States Government Accountability Office

GAO

Report to the Ranking Member, Committee on Finance, U.S. Senate

October 2010

INFORMATION SECURITY

National Archives and Records Administration Needs to Implement Key Program Elements and Controls

GAO-11-20

October 2010

INFORMATION SECURITY

National Archives and Records Administration Needs to Implement Key Program Elements and Controls

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-11-20, a report to the Ranking Member, Committee on Finance, U.S. Senate

Why GAO Did This Study

The National Archives and Records Administration (NARA) is responsible for preserving access to government documents and other records of historical significance and overseeing records management throughout the federal government. NARA relies on the use of information systems to receive, process, store, and track government records. As such, NARA is tasked with preserving and maintaining access to increasing volumes of electronic records.

GAO was asked to determine whether NARA has effectively implemented appropriate information security controls to protect the confidentiality, integrity, and availability of the information and systems that support its mission. To do this, GAO tested security controls over NARA's key networks and systems; reviewed policies, plans, and reports; and interviewed officials at nine sites.

What GAO Recommends

GAO is making 11 recommendations to the Archivist of the United States to implement elements of NARA's information security program. In commenting on a draft of this report, the Archivist generally concurred with GAO's recommendations but disagreed with some of the report's findings. GAO continues to believe that the findings are valid.

View GAO-11-20 or key components. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov and Dr. Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov.

What GAO Found

NARA has not effectively implemented information security controls to sufficiently protect the confidentiality, integrity, and availability of the information and systems that support its mission. Although it has developed a policy for granting or denying access rights to its resources, employed mechanisms to prevent and respond to security breaches, and made use of encryption technologies to protect sensitive data, significant weaknesses pervade its systems. NARA did not fully implement access controls, which are designed to prevent, limit, and detect unauthorized access to computing resources, programs, information, and facilities. Specifically, the agency did not always (1) protect the boundaries of its networks by, for example, ensuring that all incoming traffic was inspected by a firewall; (2) enforce strong policies for identifying and authenticating users by, for example, requiring the use of complex (i.e., not easily guessed) passwords; (3) limit users' access to systems to what was required for them to perform their official duties; (4) ensure that sensitive information, such as passwords for system administration, was encrypted so as not to be easily readable by potentially malicious individuals; (5) keep logs of network activity or monitor all parts of its networks for possible security incidents; and (6) implement physical controls on access to its systems and information, such as securing perimeter and exterior doors and controlling visitor access to computing facilities.

In addition to weaknesses in access controls, NARA had mixed results in implementing other security controls. For example:

- NARA did not always ensure equipment used for sanitization (i.e., wiping clean of data) and disposal of media (e.g., hard drives) was tested to verify correct performance.
- NARA conducted appropriate background investigations for employees and contractors to ensure sufficient clearance requirements have been met before permitting access to information and information systems.
- NARA did not consistently segregate duties among various personnel to ensure that no one person or group can independently control all key aspects of a process or operation.

The identified weaknesses can be attributed to NARA not fully implementing key elements of its information security program. Specifically, the agency did not adequately assess risks facing its systems, consistently prepare and document security plans for its information systems, effectively ensure that all personnel were given relevant security training, effectively test systems' security controls, consistently track security incidents, and develop contingency plans for all its systems. Collectively, these weaknesses could place sensitive information, such as records containing personally identifiable information, at increased and unnecessary risk of unauthorized access, disclosure, modification, or loss.

Contents

Abbreviations

CIO	Chief Information Officer
ERA	Electronic Records Archives
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
IT	information technology
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
POA&M	plan of action and milestones
US-CERT	United States Computer Emergency Readiness Team

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

October 21, 2010

The Honorable Charles E. Grassley
Ranking Member
Committee on Finance
United States Senate

Dear Senator Grassley:

The National Archives and Records Administration (NARA) is responsible for managing and archiving government records, which increasingly involves dealing with documents that are created and stored electronically. In 2001, NARA responded to the challenge of preserving, managing, and providing access to electronic records by initiating the development of the Electronic Records Archives (ERA).

As the nation's record keeper, NARA is responsible for significant amounts of sensitive information. In 2009 NARA experienced a data breach wherein a hard drive containing data from the Clinton Administration was lost. The hard drive reportedly contained classified information and Social Security numbers of former White House staffers and visitors.

In response to your request, we conducted an evaluation of NARA's information security program. Our objective was to determine whether NARA has effectively implemented appropriate information security controls to protect the confidentiality, integrity, and availability of the information and systems that support its mission. To accomplish this objective, we examined computer security controls over networks supporting nine sites to determine whether information was safeguarded and protected from unauthorized access. We also reviewed and analyzed NARA's security policies, plans, and reports and interviewed key agency officials.

We performed this performance audit from December 2009 to October 2010, 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. See appendix I for a complete description of our objective, scope, and methodology.

Background

Information security is a critical consideration for any organization reliant on information technology (IT) and especially important for government agencies, such as NARA, where maintaining the public's trust is essential. The dramatic expansion in computer interconnectivity and the rapid increase in the use of the Internet have changed the way our government, the nation, and much of the world communicate and conduct business. Although this expansion has created many benefits for agencies in achieving their missions and providing information to the public, it also exposes federal networks and systems to various threats.

Without proper safeguards, systems are unprotected from attempts by individuals and groups with malicious intent to intrude and use the access to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks. This concern is well-founded for a number of reasons, including the dramatic increase in reports of security incidents, the ease of obtaining and using hacking tools, the steady advance in the sophistication and effectiveness of attack technology, and the dire warnings of new and more destructive attacks to come. Over the past few years, federal agencies have reported an increasing number of security incidents, many of which involved sensitive information that has been lost or stolen, including personally identifiable information, which has exposed millions of Americans to the loss of privacy, identity theft, and other financial crimes.

NARA Is a Key Steward of Federal Records

NARA is the nation's record keeper. It was created by statute as an independent agency in 1934. On July 1, 1949, the Federal Property and Administrative Services Act transferred the National Archives to the General Services Administration, and its name was changed to National Archives and Records Services. It attained independence again as an agency in October 1984 (effective April 1, 1985) and became known as the National Archives and Records Administration. NARA's mission is to ensure continuing access to essential documentation of the rights of American citizens and the actions of their government. NARA also publishes the Federal Register, stores classified materials, and plays a role in the declassification of these classified records.

The Archivist of the United States is NARA's chief administrator and has responsibilities that include providing federal agencies with guidance and assistance for records management and establishing standards for records retention. The Archivist also has overall responsibility for ensuring the confidentiality, integrity, and availability of the information and information systems that support the agency and its operations. The

Assistant Archivist for Information Services has the responsibilities of NARA's Chief Information Officer.

In fiscal year 2009, NARA's appropriation was about $459 million, while its fiscal year 2010 appropriation is about $470 million. NARA is composed of six major divisions (see table 1) that include 44 facilities such as the headquarters locations in Washington, D.C., and College Park, Maryland; presidential libraries; and regional archives nationwide.

Table 1: Major NARA Divisions

Division	Description of function
Office of Records Services, Washington, D.C.	Accessions, preserves, describes, and provides access to the historically valuable records of the three branches of the federal government in the Washington, D.C., area. The office has agencywide responsibility for records appraisal. In addition, its conservation staff serves the entire agency and also operate the Washington National Records Center at Suitland, Maryland.
Office of Regional Records Services	Accessions, preserves, describes, and provides access to the archival records of federal executive agencies that were created outside the Washington, D.C., area and the archival records of the U.S. District Courts within 13 regional archives centers nationwide, plus provides targeted assistance program to aid federal agencies with records management. The office serves as NARA liaison for the eight affiliated archives that hold NARA-owned records on behalf of NARA in their repositories around the country.
Office of Presidential Libraries	Administers a nationwide network of presidential libraries documenting each administration beginning with the Herbert Hoover Administration. Currently, the system includes 13 Presidential Libraries, Nixon Presidential Materials Staff, and Presidential Materials Staff. These are not traditional libraries, but rather repositories for preserving and making accessible the papers, records, and other historical materials of U.S. presidents. A museum is an important component of each library.
Office of the Federal Register	Publishes public laws, coordinates the functions of the Electoral College, administers the constitutional amendment process, and provides access to the official text of federal laws, presidential documents, administrative regulations, and notices.
Office of Information Services	Provides information technology services agencywide. Also manages the development of the ERA system.
Office of Administration	Operates and maintains physical security, including the transfer of classified information.

Source: NARA.

NARA Relies on Information Systems to Accomplish Its Mission

NARA depends on a number of key information systems to conduct its daily business functions and support its mission. These systems include networks, telecommunications, and specific applications. As of fiscal year 2009, NARA reported having 39 IT systems and 4 externally hosted systems. According to NARA, as part of its key transformation initiative, in 2001 the agency responded to the challenge of preserving, managing, and assessing electronic records by beginning the development of the modern Electronic Records Archives (ERA) system. This major information

system is intended to preserve and provide access to massive volumes of all types and formats of electronic records, independent of their original hardware or software. NARA plans for the system to manage the entire life cycle of electronic records, from their ingestion through preservation and dissemination to customers. We have previously made numerous recommendations to NARA to improve its acquisition and monitoring of the system.[1]

Table 2 lists examples of key NARA systems.

Table 2: Examples of Key NARA Systems

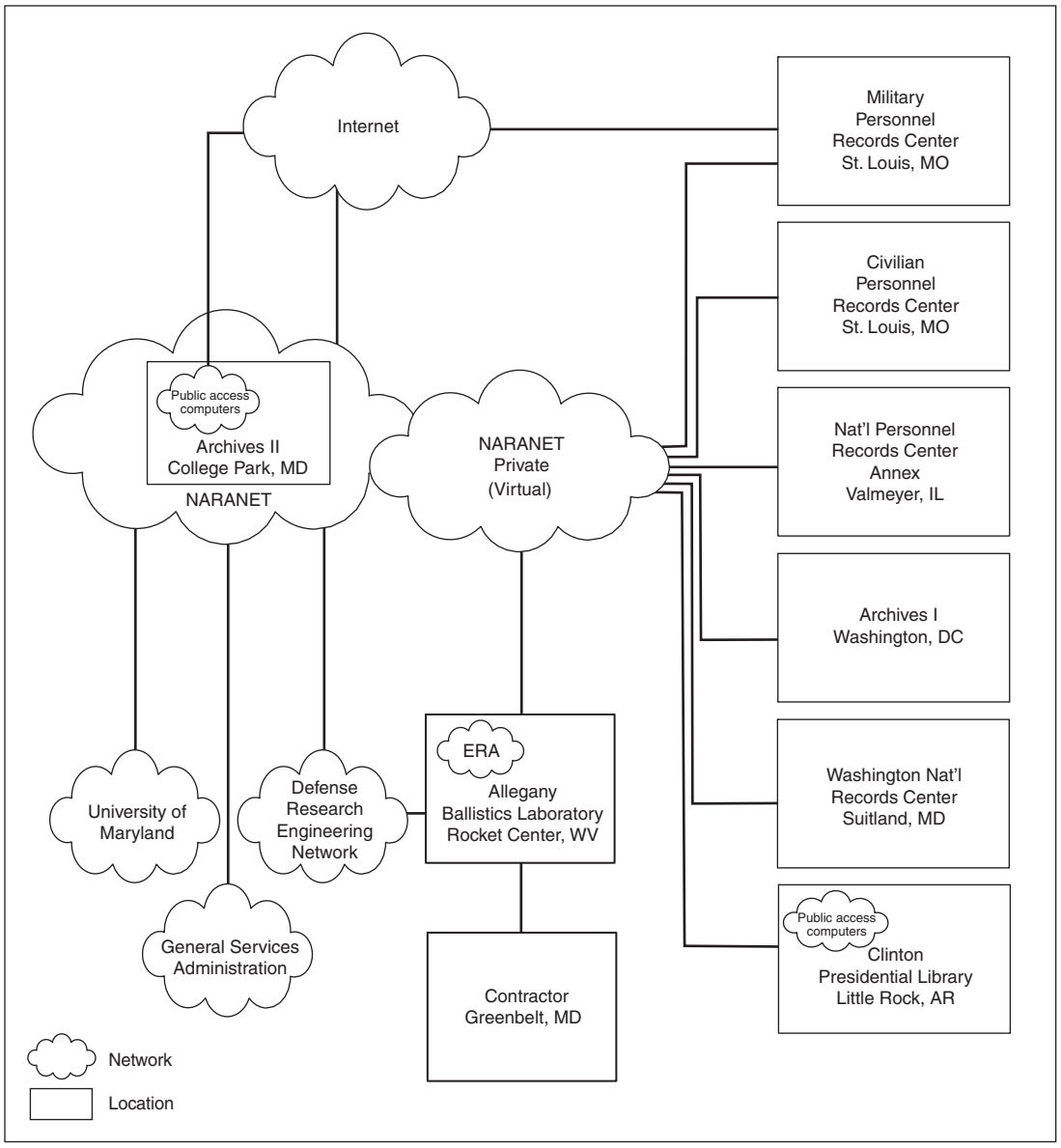
System	System location	Description
Electronic Records Archives (ERA)	Allegany Ballistics Laboratory	Plans to authentically preserve electronic records and provide discovery and delivery of archived records. A component of ERA, the Executive Office of the President system, receives, archives, and disseminates presidential holdings.
NARANET	NARA-wide	Provides data transport and processing environment for NARA's IT and application support services.
Archives Declassification Review and Redaction System (ADRRES)	Archives II	Indexes classified documents that have been withdrawn from records transferred to NARA and processes Freedom of Information Act requests for nonclassified material.
Archival Electronic Records Inspection and Control System (AERIC)	Archives II	Verifies the adequacy of the accompanying documentation for the electronic data files transferred by federal agencies to NARA.
Archival Preservation System (APS)	Archives II	Copies files from one volume to another, supports the business process of providing reference services, and provides management support for a variety of electronic records.
Archival Research Catalog (ARC)	Archives II	Provides an online catalog of NARA's holdings.
Archives and Records Centers Information System (ARCIS)	Archives II	Processes core transactions such as records transfers, accessions, dispositions, reference requests, refiles, and interfiles.
Badging and Access (B&A)	Archives II	Provides a means of transferring user information to a badge and physically reading the badge allowing or denying access depending on user access rights.
Case Management and Reporting System (CMRS)	Archives II	Automates the processing of military personnel records.
Presidential Electronic Records Library System (PERL)	Archives II	Provides a repository for electronic records produced during presidential administrations.

Source: NARA.

[1]GAO, *Electronic Records Archives: Status Update on the National Archives and Records Administration's Fiscal Year 2010 Expenditure Plan*, GAO-10-657 (Washington, D.C.: June 11, 2010).

The Office of Information Services at the Archives II facility provides centralized management and control of NARA's IT resources and services, including NARANET, the primary general support system of NARA. As shown in figure 1, NARANET is centrally located at Archives II and connects to other government and academic entities. NARANET is extended to field sites via a private network, operated by a service provider. In addition, at locations where the public has research access, NARA provides access to the Internet through the use of public access computers.

Figure 1: Simplified NARA Network Diagram



Source: GAO analysis of agency data as of July, 2010.

NARA's Information System Security Program

The Federal Information Security Management Act of 2002 (FISMA)[2] requires each federal agency to develop, document, and implement an agencywide information security program to provide security for the information and information systems that support the operations and assets of the agency, including those provided or managed by other agencies, contractors, or other sources. FISMA requires the Chief Information Officer or comparable official at federal agencies to be responsible for developing and maintaining an information security program.

The Office of Information Services centrally administers NARA's IT security program at the Archives II facility. The Assistant Archivist for Information Services, who also serves as the Chief Information Officer (CIO), is the head of the Office of Information Services. As described in table 3, NARA has designated certain senior managers or divisions at headquarters to fill the key roles in IT security designated by FISMA and agency policy.

Table 3: Positions with Key Security Responsibilities in the Office of Information Services

Position	Key responsibilities
Deputy CIO	Assists the CIO in leading the agencywide IT program and carrying out the provisions of enacted IT legislation. In coordination with the CIO, manages all day-to-day functions of the IT and information resources management program divisions and staffs.
Chief Information Security Officer	Reports to the CIO and has day-to-day oversight of NARA's information security program.
IT Security Staff	Develops and implements NARA's IT Security Program Plan and the Computer Security Response Program.
Chief Technology Officer	Directs the planning, architecture, design, and configuration management of all agencywide hardware, software, database management systems, telecommunications, data and local area and wide area networks, and related equipment and approves systems development methodologies and configuration changes to NARA's technology infrastructure.
Information Technology Services Division Director	Administers the operation of NARA's IT infrastructure, including voice and data communications systems, by NARA staff and contractors.
IT Services Branch Manager	Provides contracting officer's representative services for the Information Technology Support Systems contract, NARA's nationwide network operations contract.

[2]FISMA was enacted as title III, E-Government Act of 2002, Pub. L. No.107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002).

Position	Key responsibilities
IT Operations Branch Manager	Operates, maintains, and manages NARA's IT network infrastructure, voice and data communications systems, and IT security operations (in conjunction with IT security staff). Also monitors NARA network and desktop environments for performance.

Source: NARA.

FISMA also requires the National Institute of Standards and Technology (NIST) to provide standards and guidance to agencies on information security. NARA has a directive in place to establish its policy and guidance for information security, delineate its security program structure, and assign security responsibilities.

Control Weaknesses Threaten Record Retention

NARA has taken steps to safeguard the information and systems that support its mission. For example, it has developed a policy for granting or denying access rights to its resources, employs mechanisms to prevent and respond to security breaches, and makes use of encryption technologies to protect sensitive data.

However, security control weaknesses pervaded NARA's systems and networks, thereby jeopardizing the agency's ability to sufficiently protect the confidentiality, integrity, and availability of its information and systems. These deficiencies include those related to access controls, as well as other controls such as configuration management and segregation of duties. A key reason for these weaknesses is that NARA has not yet fully implemented its agencywide information security program to ensure that controls are appropriately designed and operating effectively. These weaknesses could affect NARA's ability to collect, process, and store critical information and records, and protect that information from risk of unauthorized use, modification, and disclosure.

NARA Did Not Fully Implement Access Controls

A basic management objective for any organization is to protect the resources that support its critical operations from unauthorized access. Organizations accomplish this by designing and implementing controls that are intended to prevent, limit, and detect unauthorized access to computing resources, programs, information, and facilities. Inadequate access controls diminish the reliability of computerized information and increase the risk of unauthorized disclosure, modification, and destruction of sensitive information and of disruption of service. Access controls include those related to (1) protection of system boundaries, (2) user identification and authentication, (3) authorization, (4) cryptography, (5)

audit and monitoring, and (6) physical security. NARA did not implement effective controls in these areas.

NARA Did Not Always Protect Network Boundaries

Boundary protection controls logical connectivity into and out of networks and controls connectivity to and from network connected devices. Unnecessary connectivity to an organization's network increases not only the number of access paths that must be managed and the complexity of the task, but the risk of unauthorized access in a shared environment. NIST guidance states that boundary protection devices should monitor and control communications at the external boundary of the system and at key internal boundaries within the system. Organizations use boundary protection devices such as proxies, gateways, routers, and firewalls to monitor and control such communications and to separate network segments that require a higher level of control than other segments of the network.

NARA has established network boundaries, but did not always adequately enforce those boundaries to secure connectivity into and out of its networks. For example, at one location, network boundaries were not adequately segregated or segmented since NARA's network was not separated from a contractor network. In addition, several internal network routers allowed direct network connections from outside the network. Similarly, firewalls at two locations were not adequately configured to control traffic into those networks, which could also allow traffic to bypass the firewalls and enter those networks. We also discovered several devices connected to a network that NARA network engineers were not aware of that could result in unidentified attacks on the network by using those devices. As a result, NARA's networks were vulnerable to unnecessary and potentially undetectable access at multiple points.

Users Were Not Always Properly Identified and Authenticated

A computer system must be able to identify and authenticate different users so that activities on the system can be linked to specific individuals. Assigning unique user accounts enables a system to distinguish one user from another (identification), while requesting specific information, such as a password, known only by a specific user allows a system to establish the validity of a user's claimed identity (authentication). The combination of identification and authentication—such as user account-password combinations—provides the basis for maintaining individual accountability and controlling access to a system. NIST states that information systems uniquely identify and authenticate users by, among other things, establishing complex (i.e., not easily guessed) passwords to reduce the likelihood of unauthorized access.

While NARA has developed a policy for identification and authentication that is based on NIST guidance, NARA has not always adequately implemented its policy. For example, multiple database systems at one location were not adequately configured to identify users and authenticate their identities when users logged in remotely. At one location, NARA also established shared, or "generic," accounts with administrator privileges on multiple systems. This practice diminishes NARA's ability to establish individual accountability and attribute system activity to a specific individual. In addition, NARA does not always enforce policies for establishing complex passwords on multiple systems and applications. As a result, increased risk exists that individuals may guess passwords and use them to gain unauthorized access to NARA's systems and networks.

Authorizations Provided Users with More Access than Necessary for Their Jobs

Authorization is the process of granting or denying access rights and permissions to a protected resource, such as a network, a system, an application, a function, or a file. A key concept for granting or denying access rights is that of "least privilege," which means that users should be granted only those access rights and permissions that they need to perform their official duties. NIST states that federal agencies should grant users only the access rights and privileges to information and information systems that are necessary for them to perform their jobs.

Although NARA has established an access control methodology based on least privilege and need-to-know principles, it has not always limited users' access rights and permissions to those necessary for them to perform their official duties. At one location, NARA provided all users on a system with read-only access to a file containing system passwords.

NARA also allowed remote root[3] (e.g., "super-user") logins to multiple servers. NARA did not disable source routing[4] on network devices. In addition, at two locations in our review, NARA granted administrator-level roles and privileges to normal user accounts for databases, which could lead to compromise of database servers. The result of these weaknesses is an increased risk of unauthorized access to NARA systems and information.

[3]Root accounts have special privileges beyond normal accounts for access to files and programs. Allowing remote login to root accounts decreases individual accountability because the root account is not tied to a specific user.

[4]Source routing is a feature that allows a packet to specify its own route, which can be helpful in several kinds of attack and should be disabled.

NARA Did Not Always Use Encryption to Effectively Protect Sensitive and Critical Information

Cryptography is a fundamental mechanism used to protect the confidentiality and integrity of critical and sensitive information. Encryption, a basic element of cryptology, involves the conversion of data into a form (cipher text) that cannot be easily understood by unauthorized individuals. This is done by transforming plain text into cipher text using a special value (a "key") and a mathematical process known as an algorithm. NIST states that federal organizations should use encryption to protect the confidentiality of remote access sessions and encrypt sessions between host systems. In addition, NIST states that organizations should encrypt passwords in storage and transmission. For encryption employed on stored information such as passwords as part of an access enforcement mechanism, the cryptography used should comply with the Federal Information Processing Standard (FIPS) 140-2, as amended, *Security Requirements for Cryptographic Modules*.[5]

NARA did not always use encryption when sensitive information was stored or transmitted. For example, at two locations, NARA used unencrypted protocols for remote management of its network, which exposed sensitive authenticating session data. In another example, unencrypted passwords for authenticating users were transmitted across NARA's network. For several systems, NARA used weak password encryption that could be easily compromised and was not compliant with FIPS 140-2 algorithms for password encryption. NARA also allowed keys (the values used to transform plain text into cipher text) to be stored unencrypted. These weaknesses unnecessarily expose critical and sensitive information to risk of unauthorized access, modification, or destruction.

Network Monitoring Was Not Consistently Implemented

To establish individual accountability, monitor compliance with security policies, and investigate security violations, it is crucial to determine what, when, and by whom specific actions have been taken on a system. To do this, organizations implement system or security software that provides an audit trail, or log, of system activity that can be used to determine the source of a transaction or attempted transaction and to monitor users' activities. Audit and monitoring technologies include network- and host-based intrusion detection systems, audit logging, security event correlation tools, and computer forensics. NIST guidance and NARA policy state that

[5]FIPS 140-2 specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information (hereafter referred to as sensitive information).

audit logs should be retained to allow monitoring of key activities, provide support for after-the-fact investigations of security incidents, and meet organizational information retention requirements.

Although NARA has many useful mechanisms at its disposal to help prevent and respond to security breaches, such as firewalls and intrusion detection systems, it has not consistently implemented integrated and responsive auditing and monitoring. At one location, audit logs for network devices did not capture sufficient levels of information and were not in compliance with NARA's 1-year retention policy for system logs. For example, over 100 network devices were not configured for remote logging, and about 65 devices did not capture information such as logs of access control lists or successful and failed login attempts. At two locations, NARA had not adequately configured auditing on several systems supporting major applications, and database systems did not archive logs in conformity with NARA's retention policy. NARA also did not have an operational program in place for detecting "rogue" access points on its wireless networks, which could allow for undetected access. As a result, NARA is limited in its ability to establish accountability, ensure compliance with security policies, and investigate violations.

Deficient Physical Security and Environmental Safety Controls Reduced Their Effectiveness

Physical security controls are a key component of limiting unauthorized access to sensitive information and information systems. These controls are important for protecting computer facilities and resources from espionage, sabotage, damage, and theft. They involve restricting physical access to computer resources and sensitive information, usually by limiting access to the buildings and rooms in which the resources are housed and periodically reviewing access rights granted to ensure that access continues to be appropriate based on established criteria. NIST states that federal organizations should implement physical security and environmental safety controls to protect employees and contractors, information systems, and the facilities in which they are located. NARA policy also requires controls for deterring and restricting physical access to areas housing sensitive IT equipment and information.

NARA effectively secured several of its sensitive areas and computer equipment and took other steps to provide physical security and environmental safety. For example, NARA issued electronic badges to help control access to many of its sensitive and restricted areas. The agency also drafted policies and procedures to guide staff in securing sensitive information and IT resources. In addition, the agency implemented several environmental and safety controls, such as temperature and humidity

controls, as well as fire protection to protect its staff and sensitive IT resources.

However, NARA has not effectively

- secured interior areas with IT equipment and sensitive information and enforced physical security safeguards;
- secured perimeter and exterior doors and controlled keys to facility doors;
- prevented and controlled unauthorized removal of sensitive information and IT components;
- authorized, authenticated, and controlled visitors to its facilities and areas containing sensitive IT equipment;
- secured locations that support computer operations; and
- environmentally protected areas containing sensitive IT equipment.

These weaknesses in NARA's physical security and environmental safety controls put sensitive information and IT resources at risk. As such, NARA facilities may be vulnerable to attack or access by unauthorized individuals, and sensitive information could be stolen, damaged, or otherwise compromised. Also, because areas containing sensitive IT and support equipment are not adequately protected, NARA has less assurance that computing resources are protected from inadvertent or deliberate misuse including sabotage, vandalism, theft, and destruction.

Weaknesses in Other Controls Increase Risk

In addition to access controls, other important controls should be in place to ensure the confidentiality, integrity, and availability of an organization's information. These controls include policies, procedures, and techniques for securely configuring information systems, sufficiently disposing of media, implementing personnel security, and segregating incompatible duties. Weaknesses in these areas increase the risk of unauthorized use, disclosure, modification, or loss of sensitive information and information systems supporting NARA's mission.

Configuration Management Controls Were Not Sufficient

One of the purposes of configuration management is to establish and maintain the integrity of an organization's work products. It involves identifying and managing security features for all hardware, software, and firmware components of an information system at a given point and

systematically controlling changes to that configuration during the system's life cycle. By implementing configuration management and establishing and maintaining baseline configurations and monitoring changes to these configurations, organizations can better ensure that only authorized applications and programs are placed into operation. NARA policy requires the most restrictive mode possible of the security settings of information technology products. NIST standards state and NARA policy requires system changes to be controlled. Patch management is an additional component of configuration management, and is an important factor in mitigating software vulnerability risks. Up-to-date patch installation can help diminish vulnerabilities associated with flaws in software code. NIST states that organizations should promptly install newly released security relevant patches, service packs, and hot fixes and test them for effectiveness and potential side effects on the organization's information systems.

NARA had not securely configured several of its systems. For example, network configurations were not always restricted in accordance with best practices; additionally, Web applications and operating systems were not always restricted in accordance with NIST guidance.

While NARA has maintained and tracked configuration changes for its ERA system, it has not consistently documented the status of those changes. NARA documented, maintained, and tracked approvals for ERA's system change requests in its meeting minutes as well as in a system for managing those change requests, but the information in meeting minutes and the change repository were inconsistent. For example, change requests agreed to in meeting minutes from October 2009 to March 2010 did not always match those entered in the repository storing those changes. Specifically, some change requests were approved for implementation in the meeting, but were listed in the repository as closed. Others were reflected as being on hold, but were actually listed as canceled in the repository. According to ERA configuration management staff, these inconsistencies exist because the configuration control board status represents a single point in time of each change request. Subsequent changes to the system related to each change request are handled by release management staff. Therefore, the status in the repository will continue to change. Configuration management staff have the responsibility to document updates to changes in status at various points in the process.

In addition, NARA had not implemented an effective patch management program for the systems we reviewed. For example, patches had not been

consistently applied to critical systems or applications in a timely manner. Specifically, several critical systems had not been patched or were out of date, some of which had known vulnerabilities. Additionally, NARA used out-of-date or unsupported software and products in some instances.

As a result of these control deficiencies, increased risk exists that the integrity of NARA systems could be compromised.

NARA Did Not Consistently Test Equipment Used to Sanitize Media

Media destruction and disposal is key to ensuring confidentiality of information. Media can include magnetic tapes, optical disks (such as compact disks), and hard drives. Organizations safeguard used media to ensure that the information they contain is appropriately controlled. Media that is improperly disposed of can lead to the inappropriate or inadvertent disclosure of an agency's sensitive information or the personally identifiable information of its employees and customers. NARA uses degaussers[6] to remove sensitive information from hard drives and tapes before reuse or destruction. This equipment should then be certified that it was tested and that it performed correctly. NIST recommends that organizations test sanitization[7] equipment and procedures to verify correct performance. NARA's policy for protection of media requires that sanitization equipment be tested annually.

However, NARA has not always ensured that equipment used for removing sensitive information was tested annually. For example, while the degausser located at one location was certified annually, one at another location was not. Specifically, one degausser was certified on January 2010, while the other had not been certified since July 2008, about 20 months prior to our on-site visit. By not testing and certifying its degausser, NARA has reduced assurance that the equipment is performing according to certified requirements.

Personnel Security Controls Are in Place

The greatest harm or disruption to a system comes from the actions, both intentional and unintentional, of individuals. These intentional and unintentional actions can be reduced through the implementation of personnel security controls. According to NIST, personnel security

[6]A degausser is a device that generates a magnetic field used to sanitize magnetic media.

[7]The process of removing sensitive information from computer media is often referred to as sanitization. It includes removing all labels, markings, and activity logs. NIST Guidelines for Media Sanitization, Special Publication 800-88 (Gaithersburg, Md., September 2006), provides guidance on appropriate sanitization equipment, techniques, and procedures.

controls help organizations ensure that individuals occupying positions of responsibility (including third-party service providers) are trustworthy and meet established security criteria for those positions. For employees and contractors assigned to work with confidential information, confidentiality, nondisclosure, or security access agreements specify required precautions, acts of unauthorized disclosure, contractual rights, and obligations during employment and after termination. NARA's security policy for personnel screening states that the type of investigation is based on the sensitivity of the position to be held.

NARA conducted the appropriate background investigations for the employees and contractors we reviewed. These individuals also had appropriate nondisclosure agreements signed when applicable to their position. However, at one location contractors had not signed nondisclosure agreements for the ERA system. NARA staff acknowledged the issue and subsequently had the contractors sign the nondisclosure agreements.

Incompatible Duties Were Not Always Effectively Segregated

Segregation of duties refers to the policies, procedures, and organizational structures that help ensure that no single individual can independently control all key aspects of a process or computer-related operation and thereby gain unauthorized access to assets or records. Often, organizations achieve segregation of duties by dividing responsibilities among two or more individuals or organizational groups. This diminishes the likelihood that errors and wrongful acts will go undetected, because the activities of one individual or group will serve as a check on the activities of the other. Effective segregation of duties includes segregating incompatible duties and maintaining formal operating procedures, supervision, and review. Inadequate segregation of duties increases the risk that erroneous or fraudulent transactions could be processed, improper program changes implemented, and computer resources damaged or destroyed. For systems categorized as high or moderate impact,[8] NIST states that incompatible duties should be segregated, such as, by not allowing security personnel who administer system access

[8]NIST Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, defines three impact levels where the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect (low), a serious adverse effect (moderate), or a severe or catastrophic adverse effect (high) on organizational operations, organizational assets, or individuals.

control functions to administer audit functions. NARA also has a policy requiring segregation of duties.

NARA did not always implement effective segregation of duties controls. For example, two staff members were each assigned security and system administration roles and responsibilities, as either a primary or backup for the ERA system (a high impact system). In addition, those individuals had privileges that allowed them to delete logs generated by the system used for auditing and logging security events. According to NARA staff, periodic reviews of the administrators' access were performed using checklists that require administrators to review each other's access activities. However at the time of our review, NARA had not documented its oversight process to ensure controls for separation of duties were implemented appropriately. As a result, NARA may face an increased risk that improper program changes or activities could go unnoticed.

NARA Has Not Fully Implemented All Elements of Its Information Security Program

A key reason for the weaknesses in information security controls intended to protect NARA's systems is that the agency has not yet fully implemented its agencywide information security program to ensure that controls are effectively established and maintained. FISMA requires each agency to develop, document, and implement an information security program that, among other things, includes

- periodic assessments of the risk and the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems;
- policies and procedures that (1) are based on risk assessments, (2) cost-effectively reduce risks, (3) ensure that information security is addressed throughout the life cycle of each system, and (4) ensure compliance with applicable requirements;
- plans for providing adequate information security for networks, facilities, and systems;
- security awareness training to inform personnel of information security risks and of their responsibilities for complying with agency policies and procedures, as well as training personnel with significant security responsibilities for information security;
- periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, which is to be performed with a

frequency depending on risk, but no less than annually, and which includes testing the management, operational, and technical controls for every system identified in the agency's required inventory of major information systems;

- a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in its information security policies, procedures, or practices;
- procedures for detecting, reporting, and responding to security incidents; and
- plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

Although NARA has developed and documented a framework for its information security program, key components of the program have not been fully or consistently implemented.

NARA Developed Risk Assessments but Inconsistently Implemented Risk-Related Procedures

In order for agencies to determine what security controls are needed to protect their information resources, they must first identify and assess their information security risks. FIPS publication 199 provides risk-based criteria to identify and categorize information and information systems based on their impact to the organization's mission.[9] In addition, the Office of Management and Budget (OMB) states that a risk-based approach is required to determine adequate security, and it encourages agencies to consider major risk factors, such as the value of the system or application, threats, vulnerabilities, and the effectiveness of current or proposed safeguards. By increasing awareness of risks, these assessments can generate support for policies and controls. NIST states that organizations should also assess physical security risks to their facilities when they perform required risk assessments of their information systems. Federal standards[10] require that NARA conduct vulnerability risk assessments at least every 3 years for the buildings and facilities we visited.

[9]NIST, *Standards for Security Categorization of Federal Information and Information Systems*, FIPS Publication 199 (Gaithersburg, Md., February 2004).

[10]According to the Federal Interagency Security Committee Standard "Facility Security Level Determinations for Federal Facilities," federal organizations are required to perform risk assessments at least every 3 to 5 years, depending on the level of the facility. Facilities visited at NARA were rated at a level requiring a frequency of at least 3 years.

NARA has developed and conducted risk assessments, but has not consistently documented risk or assessed risk in a timely manner at its facilities. For example, NARA had developed risk assessments for all 10 of the systems in our review, but other system documentation for 4 of the 10 systems cited FIPS 199 impact levels that did not match those listed in NARA's systems inventory. Documents for 3 systems reflected impact ratings higher than those listed in the systems inventory and the fourth one reflected a lower rating. Similarly, while NARA had conducted physical security risk assessments for the sites we reviewed, several had not been conducted within the required 3-year time frame. As a result, NARA may not have assurance that adequate controls are in place to protect its information and information systems.

NARA's Policies and Procedures Were Not Always Consistent with Federal Guidance

Another key element of an effective information security program is to develop, document, and implement risk-based policies, procedures, and technical standards that govern security over an agency's computing environment. FISMA requires agencies to develop and implement policies and procedures to support an effective information security program. If properly implemented, policies and procedures should help reduce the risk that could come from unauthorized access or disruption of services. Developing, documenting, and implementing security policies are the primary mechanisms by which management communicates its views and requirements; these policies also serve as the basis for adopting specific procedures and technical controls.

NARA has developed information security policies and procedures that are based on NIST guidelines. For example, NARA has developed individual policy documents that address all of the families of controls listed in NIST Special Publication 800-53.[11] To illustrate, NARA has developed information security methodologies that correspond to the controls required by NIST in the areas of access controls, configuration management, contingency planning, and security awareness training.

However, NARA's policies and procedures were not always consistent with NIST guidance. For example, NARA has not always prescribed controls based on the system's impact. NIST requires organizations to determine their information systems' impact using the security objectives of confidentiality, integrity, and availability and states that this information

[11]NIST, *Recommended Security Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 3 (Gaithersburg, Md., August 2009).

system impact level must be determined prior to the consideration of minimum security requirements and the selection of security controls for those information systems. Instead, NARA prescribed controls based on individual security objectives without taking into consideration the predetermined impact level (based on the three security objectives) of an individual system. To illustrate, NARA's access control policy only specifies controls for systems with moderate or high confidentiality, rather than suggesting controls according to the impact of the system, as determined by all three security objectives. Similarly, NARA's certification and accreditation and contingency planning methodologies prescribed controls for systems with moderate or high integrity and availability, respectively, and not based on the impact level of the system. As a result, NARA's policy may not provide the information needed to ensure that appropriate systems controls are selected that protect its information systems.

Security Plans Contained Varying Levels of Information and Did Not Always Address Required Controls

An objective of system security planning is to improve the protection of information technology resources. A system security plan provides an overview of the system's security requirements and describes the controls that are in place—or planned—to meet those requirements. OMB Circular No. A-130 requires that agencies develop system security plans for major applications and general support systems, and that these plans address policies and procedures for providing management, operational, and technical controls.[12] NIST Special Publication 800-53 states that the security plan should be updated to address changes to the system, its environment of operation, or problems identified during plan implementation or security control assessments. One of the controls recommended by NIST Special Publication 800-53 is the development of an inventory of an information system's components. This inventory should, among other things, accurately reflect the current information system, be consistent with the authorized boundary of the system, and be available for review. NARA's Security Architecture Planning Methodology also outlines security responsibilities, including responsibilities for information system owners and information owners to carry out related to system security plans. This methodology in turn mandates the use of baseline controls identified by NIST in Special Publication 800-53.[13]

[12]OMB, *Management of Federal Information Resources*, Circular No. A-130 (Nov. 28, 2000).

[13]NIST, *Recommended Security Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 3 (Gaithersburg, Md., August 2009).

NARA prepared and documented security plans for the 10 systems and networks we reviewed. All system security plans that we reviewed, with the exception of NARANET's wireless plan, identified management, technical, and operational controls, in accordance with NIST guidance and NARA policy.

However, NARA did not always include required controls in its system security plans. For example, 7 of the 13 system security plans[14] reviewed did not include a system component inventory or address where that inventory could be found. In addition, NARA has not updated its badge and access system security plan since 2003, despite replacing the system in 2007. NARA had scheduled to correct this weakness by the end of 2009, but as of September 2010 it had not been corrected. Further, NARA system security plans varied in documenting security roles and responsibilities for key individuals. Some plans were missing one or more assignments for these roles. Specifically, 6 of the 13 plans did not have the required information system owner role identified, and none of the plans reviewed had the information owner role identified or assigned.

By not addressing inventory control and assigning key security responsibilities in the system security plan, NARA increases the risk that critical information may not be available to those responsible for implementing system security plans, potentially causing a misapplication of controls to the system.

Security Awareness Training and Specialized Security Training Were Not Effectively Tracked

According to FISMA, an agencywide information security program must include security awareness training for agency personnel, contractors, and other users of information systems that support the agency's operations and assets. This training must cover (1) information security risks associated with users' activities and (2) users' responsibilities in complying with agency policies and procedures designed to reduce these risks. FISMA also includes requirements for training personnel with significant responsibilities for information security. In addition, OMB requires that personnel be trained before they are granted access to systems or applications. The training is intended to ensure that personnel are aware of the system or application's rules, their responsibilities, and their expected behavior. Further, NARA policy requires that managers and

[14]NARANET has system security plans for four subcomponents: (1) the General Support System (GSS) Application Servers; (2) desktops; (3) enterprise architecture wireless; and (4) GSS file, print, and e-mail.

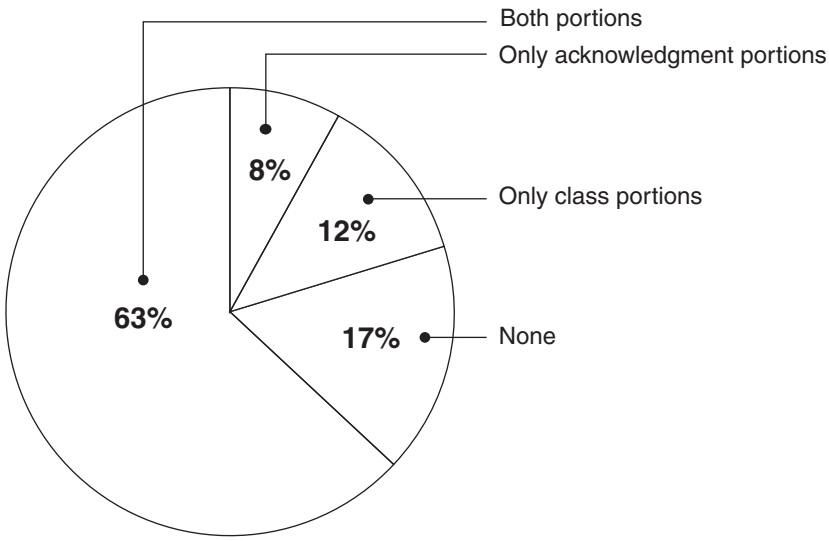
users of NARA information systems be made aware of the security risks associated with their activities and of the applicable laws, executive orders, directives, policies, standards, instructions, regulations, or procedures related to the security of NARA information systems. The policy also states that NARA must ensure that personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

NARA has a security awareness training program in place and maintains records of this training in its Learning Management System. Users are required to complete a Web-based course and, after completion, acknowledge they have reviewed and understand their security responsibilities. According to NARA's fiscal year 2009 FISMA report, the CIO reported that 100 percent of NARA's employees had received security awareness training. NARA's Inspector General concurred with this assessment. The CIO also reported that 50 employees had significant security responsibilities, and that all 50, had received specialized training. NARA's Inspector General reported a higher number stating that 114 employees had significant security responsibilities, and that 83 (73 percent) received specialized training.

However, records from NARA's training system indicated that not all users had both completed the training and acknowledged that they reviewed and understood their security responsibilities in fiscal year 2009. According to NARA's records, as of August 20, 2009, 563 of 4,536[15] individuals had completed only the class portion (12 percent) and 369 individuals (8 percent) had completed only the acknowledgment portion (although in many cases had at least started the class portion). Seven hundred and forty-nine individuals (17 percent) had not completed either portion (see fig. 2).

[15]4,536 is the total number of employees and contractors who are required to complete the security awareness training.

Figure 2: User Completion of NARA Security Awareness Training



Source: GAO analysis of NARA data.

According to NARA's Chief Information Security Officer, limitations in the training tracking system led NARA to give credit for a user interacting with the system in some way, meaning that a user who had at least started the training course received credit for the security awareness training. In addition, records of specialized security training provided by NARA indicated that 115 individuals were required to take specialized security training; of these 115, 48 (42 percent) had no record of taking specialized training. NARA officials stated that these individuals were provided with an alternate form of training to ensure their compliance with FISMA, such as a one-on-one review or an opportunity to review briefing slides.

Without an effective method for tracking that employees and contractors fully complete security awareness training, NARA has less assurance that staff are aware of the information security risks and responsibilities associated with their activities. In addition, without ensuring that all employees with specialized security responsibilities receive adequate specialized training, NARA's ability to implement security measures effectively could be limited.

NARA Did Not Fully Test Controls

A key element of an information security program is to test and evaluate policies, procedures, and controls to determine whether they are effective and operating as intended. This type of oversight is fundamental because it

demonstrates management's commitment to the security program, reminds employees of their roles and responsibilities, and identifies and mitigates areas of noncompliance and ineffectiveness. FISMA requires that the frequency of tests and evaluations of management, operational, and technical controls be based on risks and occur no less than annually. OMB requires that systems be authorized for processing at least every 3 years. NARA's policy for testing is consistent with FISMA and requires that certification testing be conducted in support of system authorizations or accreditations.

NARA had conducted tests for each of the 10 systems we reviewed; however, it had not sufficiently tested controls for 2 systems. For example, the management and operational controls for 1 system were not tested at least annually. Although NARA tested technical controls and documented test results for that system, it did not test and document the results for the system's management and operational controls. Another system had not been tested to support its accreditation since 2003. While an annual assessment was conducted in 2009 for that system, NARA's 2007 security accreditation memorandum stated that certification testing had not been performed. As a result, NARA may have reduced assurance that controls over its information and information systems are adequately implemented and operating as intended.

Remedial Action Plans Were Not Reliably Maintained

Remedial action plans, also known as plans of action and milestones (POA&M), help agencies identify and assess security weaknesses in information systems, set priorities, and monitor progress in correcting the weaknesses. NIST guidance states that each federal civilian agency must report all incidents and internally document remedial actions and their impact. POA&Ms should be updated to show progress made on current outstanding items and to incorporate the results of the continuous monitoring process. In addition, FISMA and NARA policy require the agency CIO to report annually to the agency head on the effectiveness of the agency information security program, including progress on remedial actions.

NARA has implemented a remedial action process to assess and correct security weaknesses. The format for its system-level POA&Ms includes the types of information specified in NIST and OMB guidance, such as a description of the weakness, resources required to mitigate it, scheduled completion date, the review that identified the weakness, and the status of corrective actions (ongoing or completed).

Although NARA has developed POA&Ms to address known weaknesses, the agency does not always update these plans or complete remedial actions in a timely manner. For example, a POA&M for a system designed to receive, preserve, and provide access to electronic records is dated December 2008. None of the remedial actions described in this plan were marked as completed as of April 2010. Additionally, 8 of 10 POA&Ms that we assessed contained blank entries or "to be determined" notations for some required information. These 8 did not provide all of the information for resources needed, scheduled completion dates, milestones, or the security review that identified the weakness.

In addition, a POA&M maintained by the Office of Information Services did not include information about resources required to correct these weaknesses. This lack of information about resource requirements may inhibit the agency's efforts to correct the security weaknesses. Outdated and incomplete POA&Ms compromise the ability of the CIO and other NARA officials to track, assess, and report accurately the status of the agency's information security.

Security Incident Tracking Was Inconsistent

Although strong controls may not block all intrusions and misuse, agencies can reduce the risks associated with such events if they take steps to detect and respond to them before significant damage occurs. Accounting for and analyzing security problems and incidents are also effective ways for an agency to improve its understanding of threats and the potential costs of security incidents, and doing so can pinpoint vulnerabilities that need to be addressed so that they are not exploited again. FISMA requires that each federal agency implement an information security program that includes procedures for detecting, reporting, and responding to security incidents. When incidents occur, agencies are to notify the federal information security incident center—the United States Computer Emergency Readiness Team (US-CERT).

NARA has an incident response methodology and maintains an incident database with information about the categorization and analysis of incidents. However, NARA was not able to locate all of its weekly reports for incidents and did not consistently apply its criteria for incident categorization. According to the NARA incident response methodology, incidents involving the disclosures of personally identifiable information, even if the disclosure did not involve an IT system, should be categorized under "Investigation" (Category 6). While the records indicate that NARA reported these disclosures to US-CERT, NARA did not list them as Category 6.

NARA also categorized many of its computer security incidents inconsistently. Of 640 total incidents, 139 were classified as "Explained Anomaly" (Category 7). According to the NARA incident response methodology, this category is usually reserved for false positives and other explained anomalies. However, NARA classified a number of incidents in this category, even when the incident was not a false positive or could have been placed into another category. For example, NARA experienced site-redirection events—where a user was unwittingly directed to a malicious Web site while trying to access a legitimate site. This is a form of social engineering, which is categorized in the NARA incident response methodology under a separate category (Category 5). In addition, incidents where encrypted laptops were stolen were included in the "Explained Anomaly" category, though the NARA incident response methodology indicates that they should have been placed in Category 1, which indicates that unauthorized access may have occurred.

NARA policy requires that staff be assigned and trained for the incident response team. While NARA tracks information security incidents and their resolution, it has not formally tracked training held for incident response. NARA officials have stated that they are in the process of formalizing this training program. Without ensuring that incident response personnel have received appropriate training, NARA's ability to implement security measures effectively could be limited. Further, without categorizing incidents appropriately, NARA's ability to analyze incidents for follow-on actions could be diminished, and corrective actions for protecting agency resources may not be taken.

Contingency Plans Were Developed for Most Systems

Contingency planning is a critical component of information protection. If normal operations are interrupted, network managers must be able to detect, mitigate, and recover from service disruptions while preserving access to vital information. Therefore, a contingency plan details emergency response, backup operations, and disaster recovery for information systems. It is important that these plans be clearly documented, communicated to potentially affected staff, updated to reflect current operations, and regularly tested. Moreover, if contingency planning controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which can lead to financial losses, expensive recovery efforts, and inaccurate or incomplete information.

FISMA requires each agency to develop, document, and implement plans and procedures to ensure continuity of operations for information systems that support the agency's operations and assets. Both NIST and NARA

require that contingency plans be developed and tested for information systems.

NARA developed contingency plans for 9 of the 10 systems we reviewed. Further, NARA had tested each of the contingency plans. However, a contingency plan was not developed for a system key to tracking physical records. NARA identified this weakness, but had not corrected it during the time of our review. Although all the systems in our review were tested for contingencies, NARA has less assurance that it can appropriately recover a key system in a timely manner from certain service disruptions.

Conclusions

NARA has taken important steps in implementing controls to protect the information and systems that support its mission. However, significant weaknesses in access controls and other information security controls exist that impair its ability to ensure the confidentiality, integrity, and availability of the information and systems supporting its mission. The key reason for many of the weaknesses is that NARA has not yet fully implemented elements of its information security program to ensure that effective controls are established and maintained. Effective implementation of such a program includes establishing appropriate policies and procedures, providing security awareness training, responding to incidents, and ensuring continuity of operations. Ensuring that NARA implements key information security practices and controls also requires effective management oversight and monitoring. However, until NARA implements these controls, it will have limited assurance that its information and information systems are adequately protected against unauthorized access, disclosure, modification, or loss.

Recommendations for Executive Action

To help establish an effective information security program for NARA's information and information systems, we recommend that the Archivist of the United States take the following 11 actions:

- Update NARA's system documentation and inventory to reflect accurate FIPS 199 categorizations.
- Conduct physical security risk assessments of NARA's buildings and facilities based on facility-level and federal requirements.

- Revise NARA's IT security methodologies, including those for access controls, certification and accreditation, and contingency planning, to include NIST's minimum system control requirements.
- Include inventory information and roles and responsibilities assignments in system security plans.
- Improve NARA's training process to ensure that all required personnel meet security awareness training requirements.
- Implement a process that ensures all required NARA personnel with significant security responsibilities meet specialized training requirements.
- Test management, operational, and technical controls for all systems at least annually.
- Conduct certification testing when authorizing systems to operate.
- Update remedial action plans in a timely manner and include required resources necessary for mitigating weaknesses, scheduled completion dates, milestones, and how weaknesses were identified.
- Improve the incident tracking process to ensure that incidents are appropriately categorized and that personnel responsible for tracking and reporting incidents are trained.
- Develop a contingency plan for the system that tracks physical records.

In a separate upcoming report with limited distribution, we plan to make 213 recommendations to enhance NARA's access controls to address the 142 weaknesses identified during this audit.

Agency Comments and Our Evaluation

In providing written comments on a draft of this report (reprinted in app. III), the Archivist of the United States stated that he was pleased with the positive recognition of NARA's efforts and that he generally concurred with our recommendations. NARA also provided technical comments, which we have incorporated as appropriate.

In addition, the Archivist in his comments disagreed with three of the report's findings. First, he disagreed that NARA's risk assessments in its systems inventory were incorrectly applied. However, our finding does not state that the risk assessments were incorrectly applied. Rather, as we

discuss in the report, NARA system documentation and system inventories do not consistently reflect the FIPS 199 impact levels of its systems. These inconsistencies may reduce NARA's assurance that adequate controls are in place to protect its information and information systems. Thus, we continue to believe our finding is appropriate.

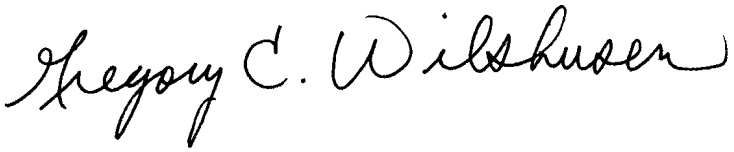
Secondly, the Archivist disagreed that NARA policies and procedures were not always consistent with NIST guidance. As we discuss in our report, NIST states that an agency must first determine the security category of its information systems and then apply the appropriately tailored set of baseline security controls. However, NARA's policy prescribed controls based on the individual security objectives of confidentiality, integrity, and availability instead of applying controls based on a prior determination of the system's impact. We believe that without first identifying the impact of the system, NARA's policy may not provide the information needed to ensure that appropriate systems controls are selected that protect its information systems. Thus, we continue to believe our finding is valid.

Lastly, the Archivist disagreed that the information owner role must be identified in each system security plan. However, NARA's policy as discussed in the report outlines key individual roles and responsibilities, including the information owner, which should be assigned for each system. By not clearly and consistently assigning these roles, NARA increases the risk that critical information may not be available to those responsible for implementing system security plans. Thus, we continue to believe our finding is valid.

As we agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution of it until 30 days from the date of this letter. At that time, we will send copies of this report to interested congressional committees and to the Archivist of the United States. In addition, this report will be available at no charge on the GAO Web site at http://www.gao.gov.

If you have any questions about this report, please contact Gregory C. Wilshusen at (202) 512-6244 or Dr. Nabajyoti Barkakati at (202) 512-4499. We can also be reached by e-mail at wilshuseng@gao.gov or barkakatin@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix IV.

Sincerely yours,



Gregory C. Wilshusen
Director, Information Security Issues

Dr. Nabajyoti Barkakati
Chief Technologist

Appendix I: Objective, Scope, and Methodology

The objective of our review was to determine whether the National Archives and Records Administration (NARA) has effectively implemented appropriate information security controls to protect the confidentiality, integrity, and availability of the information and systems that support its mission.

To determine the effectiveness of security controls, we gained an understanding of the overall network control environment, identified interconnectivity and control points, and examined controls for NARA's networks and facilities. Using our *Federal Information System Controls Audit Manual*[1] which contains guidance for reviewing information system controls that affect the confidentiality, integrity, and availability of computerized information; National Security Agency guidance; National Institute of Standards and Technology (NIST) standards and guidance; and NARA's policies, procedures, practices, and standards, we evaluated these controls by

- reviewing network access paths to determine if boundaries were adequately protected;
- reviewing the complexity and expiration of password settings to determine if password management was enforced;
- analyzing users' system authorizations to determine whether they had more permission than necessary to perform their assigned functions;
- observing methods for providing secure data transmissions across the network to determine whether sensitive data were being encrypted;
- reviewing software security settings to determine if modifications of sensitive or critical system resources were monitored and logged;
- observing physical access controls over unclassified and classified areas to determine if computer facilities and resources were being protected from espionage, sabotage, damage, and theft;
- examining configuration settings and access controls for routers, network management servers, switches, and firewalls;

[1]GAO, *Federal Information System Controls Audit Manual (FISCAM)*, GAO-09-232G (Washington D.C.: February 2009).

- inspecting key servers and workstations to determine if critical patches had been installed and/or were up to date;
- reviewing media handling policy, procedures, and equipment to determine if sensitive data were cleared from digital media before media were disposed of or reused;
- reviewing nondisclosure agreements at select locations to determine if they are required for personnel with access to sensitive information; and
- examining access roles and responsibilities to determine whether incompatible functions were segregated among different individuals.

Using the requirements identified by the Federal Information Security Management Act of 2002 (FISMA), which establishes key elements of an agencywide information security program, and associated NIST guidelines and NARA requirements, we evaluated the effectiveness of NARA's implementation of its security program by

- reviewing NARA's risk assessment process and risk assessments for 10 systems to determine whether risks and threats were documented consistent with federal guidance;
- analyzing NARA policies, procedures, practices, and standards to determine their effectiveness in providing guidance to personnel responsible for securing information and information systems;
- analyzing security plans for 10 out of 43 systems to determine if management, operational, and technical controls were in place or planned and whether security plans reflected the current environment;
- examining the security awareness training process for employees and contractors to determine if they received training prior to system access;
- examining training records for personnel with significant responsibilities to determine if they received training commensurate with those responsibilities;
- analyzing NARA's procedures and results for testing and evaluating security controls to determine whether management, operational, and technical controls were sufficiently tested at least annually and based on risk;

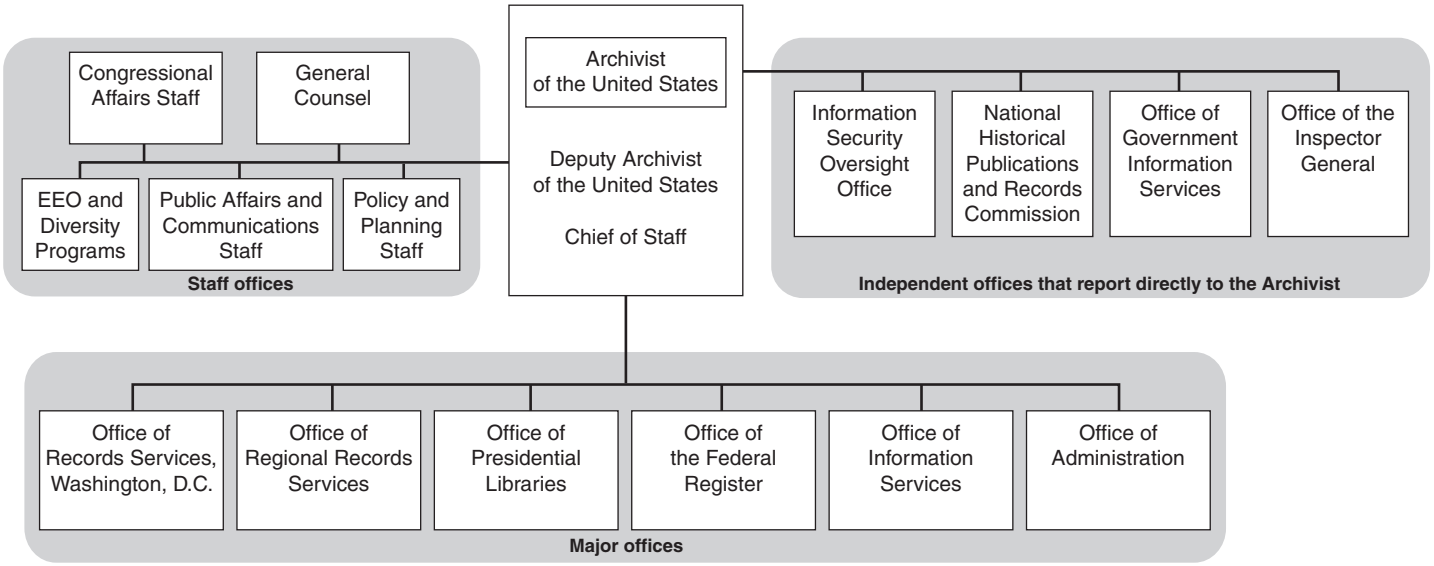
- evaluating NARA's process to correct weaknesses and determining whether remedial action plans complied with federal guidance;
- reviewing incident detection and handling policies, procedures, and reports to determine the effectiveness of the incident handling program;
- examining contingency plans for 10 systems to determine whether those plans were developed and tested; and
- reviewing three IT contracts to determine if security requirements were included.

We also discussed with key security representatives and management officials whether information security controls were in place, adequately designed, and operating effectively.

To establish the reliability of NARA's computer-processed data we performed an assessment. We evaluated the materiality of the data to our audit objectives and proceeded to assess the data by various means including: reviewing related documents, interviewing knowledgeable agency officials, and reviewing internal controls. Through a combination of methods we concluded that the data were sufficiently reliable for the purposes of our work.

We conducted this performance audit from December 2009 to October 2010 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Appendix II: NARA Organizational Chart



Source: NARA.

Appendix III: Comments from the National Archives and Records Administration

NATIONAL ARCHIVES

ARCHIVIST *of the* UNITED STATES

DAVID S. FERRIERO
T: 202.357.5900
F: 202.357.5901
david.ferriero@nara.gov

Via messenger

October 5, 2010

Gregory C. Wilshusen
Director, Information Security Issues
United States Government Accountability Office
44 G Street, NW
Washington, DC 20548

Dear Mr. Wilshusen,

Thank you for the opportunity to review and comment on the draft report entitled *INFORMATION SECURITY: National Archives and Records Administration Needs to Implement Key Program Elements and Controls.* We are pleased to note the positive recognition of our efforts by the audit staff for this engagement. We also appreciate their willingness to work with us on fine tuning some of the language in the draft report, specifically regarding technical nuances. Finally, we agree that more action is needed.

We disagree with certain findings in this report, specifically:

- that our risk assessments in systems inventory are incorrectly applied (see page 26).
- that our policies and procedures are not always consistent with NIST guidance (see page 27); and
- that the "owner role" must be identified in each system security plan (see page 31).

NATIONAL ARCHIVES *and* RECORDS ADMINISTRATION
700 PENNSYLVANIA AVENUE, NW
WASHINGTON, DC 20408-0001
www.archives.gov

In each case, we believe that we have demonstrated good faith efforts to keep these current, and acknowledge that sometimes things get missed. Nonetheless, we generally concur with each of the eleven recommendations.

Many changes are underway at NARA, including a staff reorganization that will help us more effectively address these and other challenges we face. We will create an action plan for internal use and provide semi-annual updates on our progress.

If you have questions regarding this information, please contact Mary Drak by email at mary.drak@nara.gov or by phone at 301-837-1668.

DAVID S. FERRIERO
Archivist of the United States

Appendix IV: GAO Contacts and Staff Acknowledgments

GAO Contacts

Gregory C. Wilshusen, (202) 512-6244, wilshuseng@gao.gov
Dr. Nabajyoti Barkakati, (202) 512-4499, barkakatin@gao.gov

Staff Acknowledgments

In addition to the individuals named above, Edward Alexander, Lon Chin, West Coile, Anjalique Lawrence, and Chris Warweg (Assistant Directors); Gary Austin; Angela Bell; Larry Crosland; Saar Dagani; Kirk Daubenspeck; Denise Fitzpatrick; Fatima Jahan; Mary Marshall; Sean Mays; Lee McCracken; Jason Porter; Michael Redfern; Richard Solaski; and Jayne Wilson made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548