NARA's Information Security Program

OIG Audit Report No. 15-01

October 27, 2014

Table of Contents

Executive Summary 3

Background 4

Objectives, Scope, Methodology 7

Audit Results 8

Appendix A – OMB's Micro Agencies' FISMA Compliance Scores 18

Appendix B – Acronyms and Abbreviations 20

Appendix C - Management's Response to the Report 21

Appendix D - Report Distribution List 22

Executive Summary

The Federal Information Security Management Act of 2002 (FISMA) established the requirement for Federal agencies to develop, implement and manage agency-wide information security programs, and provide acceptable levels of security for the information and systems that support the operations and assets of the agency. As part of our responsibilities under FISMA, the Office of the Inspector General (OIG) conducts an annual independent evaluation of the information security program and practices of the agency to determine the effectiveness of the program and practices. In Fiscal Year (FY) 2013, each agency Inspector General (IG) was asked to assess the information security programs in 11 areas and determine overall whether their agency had established a program for information security in each area.

We used the FY 2013 FISMA reporting metrics issued by the Department of Homeland Security in performing our assessment. Based upon our review, we determined that the National Archives and Records Administration (NARA) had not fully established an information security program consistent with FISMA policy. Specifically, many of the 11 program areas lacked documented policies and procedures to govern these areas. While an overarching policy existed, documented procedures to clarify how policy would be implemented were either missing, out of date, or no longer being followed. Some of the assessed areas had components and elements of a compliant information security program, while other areas remain deficient. Without adequate policy and procedures, NARA will continue to face challenges in complying with the requirements of FISMA due to the immaturity of its information security program.

We also determined that NARA has not fully implemented a risk management program for Information Technology (IT) Security. Specifically, NARA created an Enterprise Governance, Risk, and Compliance Program and issued a revised Internal Control Program directive however, NARA has not fully defined the controls, processes, monitoring, and testing plans within the IT Security program area. As a result, internal controls are at too high of a level to be useful to management in identifying, assessing, and mitigating risks.

This report contains two recommendations to assist NARA in establishing a foundational structure for future FISMA compliance.

Background

The Federal Information Security Management Act (FISMA) of 2002 (P.L. 107-347) was enacted to strengthen the security of information and systems within Federal agencies. Under FISMA, agency heads are responsible for providing information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems. Agency heads are also responsible for complying with the requirements of FISMA, related Office of Management and Budget (OMB) policies, and National Institute of Standards and Technology (NIST) procedures, standards, and guidelines.

Under FISMA, the agency Chief Information Officer (CIO) is required to designate a senior agency information security officer to head an office with the mission and resources to assist in ensuring agency compliance with FISMA, developing and maintaining an agency-wide information security program, and developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements. The policies and procedures should be designed based on periodic risk assessments and should cost-effectively reduce information security risks to an acceptable level; ensure information security is addressed throughout the life cycle of each agency information system; and ensure compliance with applicable requirements.

The OMB FY 2011 "Report to Congress on the Implementation of the FISMA of 2002," March 7, 2012, recognized cybersecurity as a very important factor for agencies to be able to provide essential services to citizens therefore, the Administration identified three FISMA priorities. These three priorities were emphasized as having the greatest utility in mitigating cybersecurity risks to agency information systems. The priority areas included:

- Trusted Internet Connections (TIC) – consolidate external telecommunication connections and ensure a set of baseline security capabilities for situational awareness and enhanced monitoring.
- Continuous Monitoring of Federal information systems – transforms the otherwise static security control assessment and authorization process into a dynamic risk mitigation program that provides essential, near real-time security status and remediation, increasing visibility into systems operations and helping security personnel make risk-management decisions based on increased situational awareness.
- Strong Authentication – passwords alone provide little security. Federal smartcard credentials, such as personal identity verification (PIV) and common

access cards provide multi-factor authentication and digital signature and encryption capabilities, authorizing users to access Federal information systems with a higher level of assurance.

OMB's FY 2013 Annual Report to Congress on the results of FISMA across Federal agencies and departments outlined progress in implementing the three Administration priorities listed above and reported an increase in government-wide averages of FISMA capabilities from FY 2012 to FY 2013, with significant improvements in areas such as the adoption of automated configuration management, remote access authentication, and email encryption.

The FY 2013 Annual Report to Congress also included a summary of Inspectors General's findings regarding their assessments of Federal information security programs. Although previous annual reports did not summarize the results from the IGs for the individual non-Chief Financial Officer (CFO) Act agencies, the FY 2013 annual report included the small and micro agencies'[1] compliance scores. Of the 38 small and micro agencies, 13 had programs in place for all eleven program areas and the other 25 agencies had at least one area for which it did not have a program. While the average score was 70% compliance for FY 2013, NARA's compliance score was 18% (see Appendix A).

According to NARA 804, "IT Systems Security," April 4, 2007, NARA develops, documents and implements an IT security program to provide oversight, monitoring, compliance assessments, and program management for the electronic information and information systems that support the operation and assets of NARA. NARA's Office of Information Services, headed by the CIO, includes an IT Security Division. The Chief Information Security Officer (CISO) is the senior agency information security officer responsible for the implementation of IT system security. The CISO directs the NARA IT Security Program with the mission and resources to assist in ensuring agency compliance with FISMA. IT Security Staff are responsible for planning and managing the IT Security program. In addition, IT Security Staff are to assist in the development of the security architecture, ensure the appropriate integration of security controls as part of the systems engineering process, and provide guidance and assistance to system owners on matters of IT security.

The OIG's annual FISMA evaluations continue to identify gaps in NARA's information security program and areas needing improvement. The OIG FISMA evaluation criteria only allows for the use of "Yes," "No," or "N/A" responses. Further, the criteria requires the OIG to determine if a program is "established" for each of the 11 program areas. The criteria specifically defines "established" as consistent implementation of defined policy

[1] A "small agency" has less than six thousand employees; most have fewer than five hundred staff. A "micro agency" has fewer than 100 employees.

and procedures. Therefore, if a program area did not have FISMA compliant policy in place or consistent implementation of such policy, the program area was determined not to be established. As shown in Table 1 below, progress in establishing an information security program has been slow and little changes have been seen over the last three years.

Table 1. Results of the FY 2013 and Previous Year's FISMA IG Evaluations

Cybersecurity Program Area	FY 2013 Results	FY 2012 Results	FY 2011 Results
	Established Program?[2]	Established Program?	Established Program?
Information Security Continuous Monitoring	No	No	No
Configuration Management	No	No	No
Identity and Access Management	No	No	No
Incident Response and Reporting	No	No	No
Risk Management	No	No	No
Security Training	No	No	No
POA&M	No	No	No
Remote Access Management	No	Yes	No
Contingency Planning	No	No	No
Contractor Systems	No	No	No
Security Capital Planning	No	No	No

[2] DHS FY 2013 IG FISMA Reporting Metrics defined "established" as consistent implementation of the defined policy and procedures.

Objectives, Scope, Methodology

This annual independent evaluation was performed as required by FISMA. The purpose was to assess the maturity of controls over information security and compliance with information security policies, procedures, standards, and guidelines. We reviewed 11 areas based on the Department of Homeland Security's FY 2013 Inspector General FISMA Reporting Metrics, issued November 30, 2012.

Our independent evaluation focused on NARA's information security program, the requirements outlined in FISMA, and the FY 2013 FISMA reporting metrics. To accomplish our objective, we assessed NARA's compliance with the security requirements mandated by FISMA and other Federal information security policies, procedures, standards, and guidelines. Specifically, we: (1) interviewed personnel and officials from Information Services and Business Support Services; (2) reviewed documentation provided by those offices to determine whether NARA had an information security program that contained the attributes identified in the OIG FISMA Reporting Metrics; and (3) obtained and reviewed an inventory of information systems from the CIO and selected a representative judgmental[3] sample of 10 of 46 systems to review.

In November 2013, the results of our independent evaluation were reported in CyberScope, the FISMA reporting application which captures the responses for each attribute and provided additional areas for narrative comments. Although NARA partially implemented some of the attributes, we answered the question as "no" because the attribute was not fully or consistently implemented. We attempted to include a comment below the metric when this occurred to qualify that NARA had implemented the control for some, but not all, systems. Based on the results of the FY 2013 evaluation and the limited progress made from previous year's evaluations, and at the request of NARA's former Chief Information Officer, the OIG chose to issue an audit report with formal recommendations to assist NARA in establishing a foundation for future FISMA compliance.

Our audit work was performed at Archives II in College Park, Maryland between July 2013 and July 2014. 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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[3] We selected a judgmental sample because we did not plan to project the results.

Audit Results

1. Information Security Program

NARA has not fully established an information security program consistent with FISMA, OMB policy, or NIST guidelines in any of the 11 program areas reviewed. NARA's difficulty in establishing an information security program can be attributed to absent or outdated policy and procedures. Specifically, while some elements of an information security program exist, NARA has not defined the policy and procedures necessary to govern these areas. FISMA requires agency CIO's to develop and maintain information security policies, procedures, and control techniques to address applicable OMB and NIST requirements. Without adequate policies and procedures, NARA will continue to face challenges in complying with the requirements of FISMA due to the immaturity of its information security program.

According to FISMA, the head of each Federal agency is responsible for ensuring senior agency officials provide information security for the information and information systems that support the operations and assets under their control. This is done in part by implementing policies and procedures to cost-effectively reduce risks to an acceptable level. FISMA allows the head of each agency to delegate to the agency CIO the authority to develop and maintain information security policies, procedures, and control techniques.

NARA has not fully established a program for information security in any of the 11 program areas reviewed. One area, Remote Access Management, was generally compliant but lacked several key attributes of an effective program. The remaining 10 program areas were not compliant with FISMA requirements and did not meet the level of performance specified by DHS due to the majority of the attributes not implemented. Specifically, while NARA had some elements in place among the program areas, other elements were only partially implemented or had not been implemented at all. The results from the FY 2013 FISMA evaluation revealed similar gaps in the information security program as the FY 2012 FISMA evaluation with little progress made.

For example, NARA's continuous monitoring program remained under development in FY 2013. According to NIST SP 800-53, continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. There were four attributes to the continuous monitoring program IGs were asked to evaluate as part of the FISMA reporting metrics:

1.1 Documented policies and procedures for continuous monitoring.
1.2 Documented strategy and plans for continuous monitoring.
1.3 Ongoing assessments of security controls (system-specific, hybrid, and common) that have been performed based on the approved continuous monitoring plans.
1.4 Provides authorizing officials and other key system officials with security status reports covering updates to security plans and security assessment reports, as well as a common and consistent POA&M program this is updated with the frequency defined in the strategy and/or plans.

NARA's continuous monitoring program did not include any of the four attributes. NARA's "IT Security Requirements," version 5.6.2, March 31, 2011, contained a high level policy statement "for all data, the NARA IT Security Staff shall establish a continuous monitoring strategy and implement a continuous monitoring program." However, procedures had not been developed and a documented strategy and continuous monitoring plan were still under development in FY 2013. Assessments conducted were targeted towards providing information for three areas needed for the CIO's FISMA reporting metrics. In addition, NARA's authorizing official, the CIO, did not receive regular security status reports and system POA&Ms were not updated to reflect control failures identified during the security control assessments.

Among the 11 program areas, DHS FISMA Reporting Metrics included 99 attributes for OIG's to evaluate. Of the 99 attributes, NARA had only implemented 26. Table 2 provides a summary, by program area, of the attributes missing from its information security program.

Table 2. Summary of Key Missing Attributes in NARA's Information Security Program

Continuous Monitoring:
• Documented procedures were still under development. • NARA had not established a strategy or plan to implement continuous monitoring. • NARA did not have an approved continuous monitoring plan. • The CIO did not receive regular security status reports on existing systems.
Configuration Management:
• Configuration management policy and procedures were not fully developed. • NARA-approved deviations from external configuration baselines were not defined. • The capability to assess compliance with baseline configurations was only implemented for some systems. • Additional deviations to the U.S. Government Configuration Baseline (USGCB) secure configuration for Windows-based components were not documented.

Identity and Access Management:
• Documented policies and procedures exist but have not been updated. • NARA has not implemented the PIV for logical or physical access. • A process is not in place to consistently terminate or deactivate accounts once access is no longer needed.
Incident Response and Reporting:
• Policies and procedures were outdated and did not reflect NARA's current practice on capturing and reporting incidents. • Reports to US-CERT did not always meet established timeframes. • Incident monitoring and detection coverage was not sufficient.
Risk Management:
• Policies and procedures were outdated. • Comprehensive governance structure and overall risk management strategy were not fully developed[4]. • CIO did not have visibility of system-level POA&Ms. • Security control assessments were not tied to security requirements of the system. • No formal process was in place to communicate system-specific, mission/business, or organizational-level risks to appropriate levels.
Security Training:
• Policies and procedures for security training were outdated. • Security training content for users with significant security responsibilities was not based on the organization or individual roles.
Plan of Action & Milestones:
• Policies and procedures exist but have not been consistently implemented across NARA. • POA&M elements were outdated, not prioritized, and/or did not have information on the owner, required resources, and scheduled completion dates. • A process was not in place to regularly update the CIO on system-level POA&Ms to ensure proper monitoring and remediation.
Remote Access Management:
• Policies and procedures for authorizing, monitoring, and controlling all methods of remote access did not exist. • Monitoring for unauthorized connections did not occur. • Lost or stolen devices may not have been disabled and appropriately reported. • A policy was not in place to detect and remove unauthorized (rogue) connections.
Contingency Planning:
• Documented policy and procedures were outdated. • Results of system Business Impact Assessments (BIA) were not incorporated into the NARA Continuity of Operations Plan (COOP), Business Continuity Plan (BCP) or

[4] Since the FISMA results were provided to OMB , NARA issued Directive 160 "Enterprise Governance, Risk, and Compliance Program," February 25, 2014, and Directive 161 "Internal Control Program," February 25, 2014, which incorporates NARA's comprehensive governance structure and overall risk management strategy.

Disaster Recovery Plan (DRP).[5] • IT infrastructure recovery plan is outdated and does not reflect the current architecture. • Testing of system specific contingency plans did not occur in FY 2013. • NARA has a Test, Training, and Exercise (TT&E) program for the COOP, but a TT&E program does not exist at the system level. • NARA did not test or exercise the Disaster Recovery Infrastructure Specification and Network Design plan. • Most systems do not have alternate processing sites.
Contractor Systems:
• Policies and procedures for oversight of systems operated by contractors or other entities were not documented. • NARA does not ensure systems operated by contractors in the public cloud continue to be compliant with organization guidelines.
Security Capital Planning:
• Capital Planning and Investment Control (CPIC) policy is no longer being followed. • Information security requirements were not always included as part of the CPIC process. • NARA's IT budget does not include a discrete line item for information security. • Information security resources required are not recorded each year. • A process is not in place to ensure information security resources are available for expenditure as planned.

Overall, we identified a lack of policy and procedures or outdated policy and procedures in all 11 program areas. NARA Directive 804 "IT Systems Security," April 4, 2007, established policy for securing all electronic information collected or maintained by or on behalf of NARA and the electronic information systems used or operated by NARA. The Directive assigned responsibilities and defined the objectives of the IT Security Program. Several supplements referenced in NARA 804 contain the specific standards and procedures for implementation of NARA IT security policy. For example, according to NARA 804, the Security Architecture Section of the Enterprise Architecture contains Methodology sections which provide detailed instructions on the implementation for each of the security control families identified in the Security Architecture.

We reviewed the Methodologies for 8 of the 11 program areas[6] and found the Methodologies had not been updated since 2011, and did not contain detailed instructions on implementing security controls. Instead, each control referred to the "NARA IT Security Requirements" document. NARA's IT Security Requirements, version 5.6.2, March 31, 2011, documents the security requirements mandated by FIPS 200 "Minimum Security Requirements for Federal Information and Information Systems," and includes

[5] NARA does not have a Business Continuity Plan or Disaster Response Plan.
[6] NARA did not have Methodology documents for two program areas: Continuous Monitoring, Contractor Systems and Security Capital Planning.

NARA tailoring to implement the control. However, formal, documented procedures to facilitate the implementation of the policy and associated controls were either missing or outdated.

For example, control CM-1 "Configuration Management Policy and Procedures," in NARA's IT Security Requirements states that for all data, the NARA Office of Information Services shall develop, disseminate, and review/update at least annually a formal, documented configuration management policy and formal documented procedures to facilitate implementation of the configuration management policy and associated configuration management controls. Neither documented policy nor documented procedures existed in FY 2013. A new Configuration Management Team was formed in FY 2013 to provide enterprise level support for configuration management. One of the team's objectives for FY 2014 was to establish agency policy, standards, and guidance for performing configuration management.

During the FISMA review, we noted that NARA uses external configuration baselines but has not documented the organization-approved deviations from those baselines. In addition, NARA has the automated capability to assess compliance with baseline configurations for some systems but not all. Several other attributes were based on whether processes had been implemented in accordance with organization policy or standards. Because NARA lacks defined configuration management policy and procedures, attributes such as whether NARA has a process for timely remediation of scan result deviations or timely remediation of configuration-related vulnerabilities, including scan findings, had not been established.

In FY 2014, the IT Security Division made some progress in developing documented procedures. For example, the NARA Information Security Continuous Monitoring Concept of Operations was finalized and a Continuous Monitoring Matrix based on NIST SP 800-53, Revision 4 controls was created to document the frequency, primary role, and output for each control test. NARA also updated the Methodology for Certification and Accreditation and Security Assessments however, at least two controls were still in the process of being updated and the standard control language from NIST SP 800-53, Rev. 4 was included in the Methodology instead of NARA's implementing procedures.

Without defined policies and procedures, NARA's information security program will not have an established program consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.

Recommendation 1

The CIO should develop new policies and procedures or update existing policies and procedures for at least the 11 program areas included in the annual FISMA review.

Management Response

Management concurred with the recommendation.

2. Risk Management and Internal Controls

NARA has not implemented an effective risk management and internal control program for IT Security. NARA is in the process of implementing a new agency-wide internal control program however, controls, processes, monitoring and testing plans associated with IT Security have not been fully identified as part of the internal control program and are not sufficiently reflected in NARA's Internal Control Program Tool. This occurred because only one function area has been defined for the IT Security program which is not reflective of the Office of Information Services' IT Security Division's work and around which risk and controls need to be assessed. According to NARA 161, "NARA's Internal Control Program," Executives are responsible for ensuring the internal control framework accurately reflects the structure and responsibilities of their office. As a result, the internal controls defined for the IT Security function are at too high of a level to be useful to management in identifying risks and determining whether mitigation strategies are needed.

In FY 2012, NARA recognized that the current Enterprise Governance, Risk Management and Compliance (EGRC) environment was ad-hoc or non-existent and no formal structure was in place around which risks and controls were assessed and managed across the agency. As a result, the Performance and Accountability Office within the Office of the Chief Operating Officer developed an overarching structure for NARA's EGRC in NARA 160, "Enterprise Governance, Risk, and Compliance Program," February 25, 2014, and issued policy and guidance for NARA's internal control program (one of three major components of EGRC program). NARA 161 "NARA's Internal Control Program," February 25, 2014, assists managers in monitoring their operations and managing risk so they can provide reasonable assurance programs and functions are operating efficiently and effectively; assets are properly safeguarded; and NARA is in compliance with laws and authorities.

According to NARA 161, at the beginning of each fiscal year, program owners and function owners must review and revise as appropriate, the programs and functions of each office to form the basis against which internal controls will be assessed for the coming fiscal year. NARA developed an internal Microsoft Access database to support automation of the internal control/risk management program. This Internal Control Program Tool was to be used for capturing and reporting on internal control responsibilities, risks, and results of periodic testing of internal controls.

We reviewed the programs and functions established in the Internal Control Program Tool for the Office of Information Services and found that controls, processes, monitoring and testing plans have not been fully identified within the IT Security function area. Specifically, the Internal Control Program for Information Services contains six program areas: IT Operations; Administration, Policy and Planning; Quality Assurance; Strategic Systems Management; IT Security; and Digital Preservation. As of July 2014, only one function area had been defined for the IT Security program: "Secure NARA IT Systems."

The single IT Security function area included four control topic areas related to Assessment and Authorization, Continuous Monitoring Concept of Operations, Plan of Action and Milestones Management, and Incident Response. Detailed descriptions of the actual controls in place for each of these topic areas were not included although each control topic had a separate indicator, process, and scheduled tests for FY 2014. For example, the Assessment and Authorization control used the indicator "percent of FISMA systems with Authority to Operate," and the process was that for new major systems at NARA, a full security assessment and authorization would be conducted for the system. Scheduled testing for FY 2014 included assessment procedures utilizing NIST 800-53a testing guidelines and automated tools to collect information on NIST 800-53 control implementation for systems. The information provided did not reflect the risks involved with the assessment and authorization process or the controls in place to mitigate the risks.

According to Office of Performance and Accountability (CP) personnel, the vast scope of IT Security creates challenges in attempting to aggregate all existing IT Security controls in one place. Further, CP cites technological challenges in performing this task due to the limited functionality of NARA's Internal Control Program Tool developed in-house. CP acknowledges the minimal amount of information concerning IT Security controls, testing, monitoring, and results currently existing in the Internal Control Program Tool does not provide sufficient evidence to reasonably ensure control objectives are being met.

Having only one function area under IT Security is not sufficient to ensure safeguarding of assets; efficient and effective operations; reliable and accurate financial data and reporting; and compliance with applicable laws and regulations. In order for NARA to ensure it is effectively and efficiently accomplishing its information security objectives, additional functional areas should be identified. In addition, the single function "Secure NARA IT Systems" should be divided into multiple function areas so that a risk assessment can be conducted for each individual area and controls can be established to address the risks identified. For example, NARA should include additional function

areas and controls needed to ensure compliance with laws and regulations such as FISMA.

FISMA specifies eight requirements of an information security program:

1) 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;
2) Policy and procedures;
3) Subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems;
4) Security awareness training;
5) Periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices;
6) A process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in information security policies, procedures, and practices of the agency;
7) Procedures for detecting, reporting, and responding to incidents; and
8) Plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

NARA's existing functional area includes the monitoring of the FISMA requirement for a process to plan, implement, evaluate and document remedial actions and also partially monitors the FISMA requirement for periodic testing and evaluation of the effectiveness of information security practices. NARA's control related to Incident Response does not capture the extent of the FISMA requirement for NARA to establish procedures for detecting, reporting, and responding to incidents. Expanding internal control information for IT Security captured by the Internal Control Program Tool would allow the CISO, CIO, and other NARA executives better visibility into the state of IT Security and provide them with better information about IT Security controls and risks on which to base decisions.

Currently internal controls defined for the IT Security function are at too high of a level to be useful to management in identifying, evaluating, and mitigating risks. Annual FISMA reviews conducted by the NARA OIG have consistently identified weaknesses within NARA's information security program. Without useful IT Security internal controls, NARA may not be able to effectively manage risks. Additionally, goals and objectives for IT Security may not be met. Therefore, it is imperative managers adequately establish, monitor, and test internal controls on an on-going basis.

Recommendation 2

The CIO should coordinate with the Office of Performance and Accountability and the Chief Operating Officer (NARA's Risk Officer) to identify, assess, capture, and report IT Security controls within NARA's Internal Control Program Tool in order to adequately ensure safeguarding of assets; efficient and effective operations; reliable and accurate financial data and reporting; and compliance with applicable laws and regulations.

Management Response

Management concurred with the recommendation.

Appendix A – FISMA Compliance Scores for Small and Micro Agencies

Agency[7]	FY 2013 (%)
Equal Employment Opportunity Commission	99%
Tennessee Valley Authority	99%
Farm Credit Administration	99%
Federal Energy Regulatory Commission	99%
Export-Import Bank of the United States	96%
Federal Housing Finance Agency	95%
Federal Trade Commission	92%
National Endowment for the Arts	92%
Merit Systems Protection Board	88%
Smithsonian Institution	88%
Federal Reserve Board	88%
National Labor Relations Board	87%
National Endowment for the Humanities	87%
Federal Deposit Insurance Corporation	87%
Federal Labor Relations Board	84%
Millennium Challenge Corporation	84%
Other Defense Civil Programs	84%
National Credit Union Administration	83%
Commodity Futures Trading Commission	81%
Railroad Retirement Board	80%
Securities and Exchange Commission	80%
National Transportation Safety Board	78%
Overseas Private Investment Corporation	74%
Corporation for National and Community Service	72%

[7] Federal Retirement Thrift Investment Board, Federal Election Commission, and Office of Special Counsel did not provide the answers with the detail required for scoring for FY 2013.

Agency[7]	FY 2013 (%)
Consumer Financial Protection Bureau	72%
Pension Benefit Guaranty Corporation	71%
Court Services and Offender Supervision Agency	71%
Federal Mediation and Conciliation Service	65%
Federal Maritime Commission	54%
International Boundary and Water Commission	53%
International Trade Commission	51%
Broadcasting Board of Governors	50%
Peace Corps	33%
Consumer Product Safety Commission	30%
National Archives and Records Administration	18%
Federal Retirement Thrift Investment Board	N/A
Federal Election Commission	N/A
Office of Special Counsel	N/A

Source: Data provided to DHS via CyberScope from October 1, 2012, to September 30, 2013.

Appendix B – Acronyms and Abbreviations

BCP	Business Continuity Plan
BIA	Business Impact Analysis
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COOP	Continuity of Operations Plan
CPIC	Capital Planning and Investment Control
DHS	Department of Homeland Security
DRP	Disaster Response Plan
EGRC	Enterprise Governance, Risk Management and Compliance
FISMA	Federal Information Security Management Act
FY	Fiscal Year
IT	Information Technology
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PIV	Personal Identity Verification
POA&M	Plan of Action and Milestones
TIC	Trusted Internet Connections
TT&E	Test, Training, and Exercise
US-CERT	U.S. Computer Emergency Response Team

Appendix C - Management's Response to the Report

NATIONAL ARCHIVES

Date: OCT 2 2 2014

To: James Springs, Acting Inspector General

From: David Ferriero, Archivist of the United States

Subject: OIG Revised Draft Audit Report 15-01, Audit of NARA's Information Security Program

Thank you for the opportunity to provide comments on this revised draft report. We appreciate your willingness to meet and clarify language in the report.

We concur with both recommendations in this audit, and we will address them further in our action plan.

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 D - Report Distribution List

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