OFFICE *of*
INSPECTOR GENERAL
NATIONAL ARCHIVES

November 4, 2016

TO: David S. Ferriero
Archivist of the United States

FROM: James Springs James Springs
Inspector General

SUBJECT: *Audit of NARA's Information System Inventory*

Attached for your action is our final report, *Audit of National Archives and Records Administration's Information System Inventory* (OIG Audit Report No. 17-AUD-02). We incorporated the formal comments provided by your office.

The report contains eight recommendations aimed at improving NARA's Information Systems Inventory. Your office concurred with the recommendations. Based on your October 18, 2016 response to the draft report, we consider all the recommendations resolved and open. Once your office has fully implemented the recommendations, please submit evidence of completion of agreed upon corrective actions so that recommendations may then be closed.

As with all OIG products, we will determine what information is publicly posted on our website from the attached report. Should you or management have any redaction suggestions based on FOIA exemptions, please submit them to my counsel within one week from the date of this letter. Should we receive no response from you or management by this timeframe, we will interpret that as confirmation NARA does not desire any redactions to the posted report.

Consistent with our responsibility under the *Inspector General Act, as amended,* we may provide copies of our report to congressional committees with oversight responsibility over the National Archives and Records Administration.

Please call me with any questions, or your staff may contact Jewel Butler, Assistant Inspector General of Audits, at (301) 837-3000.

OFFICE *of* INSPECTOR GENERAL
NATIONAL ARCHIVES

Audit of NARA's Information System Inventory

November 4, 2016

OIG Audit Report No. 17-AUD-02

Table of Contents

Executive Summary

Audit of NARA's Information System Inventory

OIG Report No. 17-AUD-02 November 4, 2016

Why Did We Conduct This Audit?

Information system inventories are the basic tools used by agencies to support information resource management processes including information technology planning, budgeting, acquisition, monitoring, testing, and evaluation of information security controls. A key goal of the inventory process is to ensure information systems are acquired/engineered, operated, and maintained to provide acceptable security. We performed this audit to determine if National Archives and Records Administration (NARA) has developed a comprehensive information system inventory to track and monitor all information systems operated or maintained throughout the agency. We also evaluated NARA's information systems to determine if they were adequately classified and categorized.

What Did We Recommend?

NARA should Develop, document, approve and implement a process for developing and maintaining the system inventory, in adherence to 44 U.S.C. § 3505(c); and comply with FIPS 199 and NIST SP 800-60 to ensure all information systems are accurately categorized.

What Did We Find?

Information Services does not maintain a comprehensive and accurate information system inventory. We found missing data fields, inaccurate information, and information systems managed by NARA personnel and contractors that were not included on NARA's master systems inventory. This occurred because Information Services has not finalized and implemented systems inventory guidance; has not documented a process for identifying information systems that should be listed on the inventory; and has not clearly defined who within Information Services is responsible for maintaining the information system inventory. Federal Law requires the head of each agency to develop and maintain an inventory of the information systems (including national security systems) operated by or under the control of such agency. Without a comprehensive and accurate systems inventory, NARA has reduced assurance information systems are adequately acquired/engineered, operated, and maintained to provide acceptable security.

In addition, NARA system owners were not adequately categorizing information systems using Federal Information Processing Standards Publication 199 (FIPS 199). Controls were not in place to ensure system owners used proper documentation to categorize the systems. System owners were either using incomplete FIPS 199 categorization documentation provided by Information Services or not using FIPS 199 at all to categorize their information system. Incorrect FIPS 199 security categorization can result in the agency either over protecting the information system thus wasting valuable security resources, or under protecting the information system and placing important operations and assets at risk. Consequently, NARA may not be 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.

James Springs

James Springs
Inspector General

Background

Under the Federal Information Security Modernization Act (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[1]. 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.

FISMA requires agencies to conduct periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually. This testing shall include testing of management, operational, and technical controls of every information system identified in the inventory required under the Paperwork Reduction Act (codified at 44 United States Code (U.S.C.) § 3505(c))[2]. A critical component of this testing is the Federal Information Processing Standards Publication 199 (FIPS 199) categorization of an information system. FIPS 199 is the process by which system owners review all of the information types within an information system to determine the overall categorization of a system. The overall categorization is then used to select the appropriate NIST Special Publication (SP) 800-53 version 4 security controls that need to be applied to the system and tested.

44 U.S.C. § 3505(c) requires the development of two different information system inventories: an inventory of major information systems as well as one with all agency information systems. Information system inventories are basic tools used to identify information systems and their boundaries. According to 44 U.S.C. § 3505(c), an inventory supports information resource management including information technology planning, budgeting, acquisition, and management as well as monitoring, testing, and evaluation of information security controls. 44 U.S.C. § 3505(c) goes on to state an inventory is supposed to identify the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency. The Chief Information Officer's (CIO) annual FISMA metrics from 2014 published by DHS stated a key goal of an inventory is to ensure systems are acquired/engineered, operated, and maintained to provide acceptable security.

[1] The term "information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

[2] FISMA simply references 44 U.S.C. § 3505(c) to define the inventory. However, there are two paragraphs labeled as (c) in section. One of these details the major information systems and the other details the complete information system inventory.

Information Services, led by NARA's CIO, oversees NARA's information technology (IT) security and applied research initiatives; manages NARA's IT management processes (e.g., Capital Planning Project Management, and Enterprise Architecture), and IT governance boards; and supports the Chief Innovation Office in meeting customers' needs for effective and innovative social media, open government, and digitization services, solutions, and systems.

Within Information Services is the Security Management Division, led by the Chief Information Security Officer, who is responsible for developing and managing an IT Security Program that includes standards and guidelines for NARA IT systems issued in accordance with law and as directed by the President. These security activities comply with applicable Federal statutes, and must align with the standards specified in the NARA IT security architecture. Another division within Information Services involved in the information system inventory is Investment Planning and Management staff. They are responsible for NARA's IT Capital Planning and Investment Control (CPIC) process. In addition, they are informally responsible for the development and maintenance of NARA's information system inventory.

Objectives, Scope, Methodology

The audit objective was to determine if NARA has developed a comprehensive information system inventory to track and monitor all information systems operated or maintained throughout NARA, and to evaluate NARA's information systems to determine if they were adequately classified and categorized. To accomplish our objective, we reviewed the following guidance:

- The Paperwork Reduction Act, 44 U.S.C. § 3505(c), "Public Printing and Documents,"
- Government Accountability Office "Standards for Internal Control in the Federal Government" (GAO Standards),
- FISMA of 2014,
- NIST SP 800-18 "Guide for Developing Security Plans for Federal Information Systems"
- NIST SP 800-53 Revision 4 "Security and Privacy Controls for Federal Information Systems and Organizations,"
- NIST SP 800-60 Volume I "Guide to Mapping Types of Information and Information Systems to Security Categories,"
- NIST SP 800-60 Volume II "Appendices to Guide to Mapping Types of Information and Information Systems to Security Categories,"
- FIPS 199 "Standards for Security Categorization of Federal Information and Information Systems," and
- NARA Directive 804 "Information Technology (IT) Systems Security."

We interviewed personnel from Information Services and Agency Services involved in information systems inventory and oversight of information systems. We obtained and analyzed internal documents relating to NARA's information system inventory and categorization processes. Finally, we conducted a survey of NARA organizations to develop a potential universe of information systems managed and operated by NARA and its contractors that could be included on NARA's inventory. We asked each organization to provide a list of the systems they manage. For each system listed, we requested a description of the system, system points of contact including the information system security officer, whether the system had Personally Identifiable Information (PII), and the system's FIPS 199 categorization level. We did not completely verify the accuracy of all the survey responses, or determine whether or not other systems should have been included in the inventory.

Our audit work was performed at Archives II in College Park, Maryland between March 2016 and May 2016. This audit was included in the Office of Inspector General's (OIG) Annual Audit Plan. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require 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.

This audit was conducted by Andrew Clements, Senior IT Auditor.

Audit Results

Finding 1. NARA's Information System Inventory Not Accurate and Complete

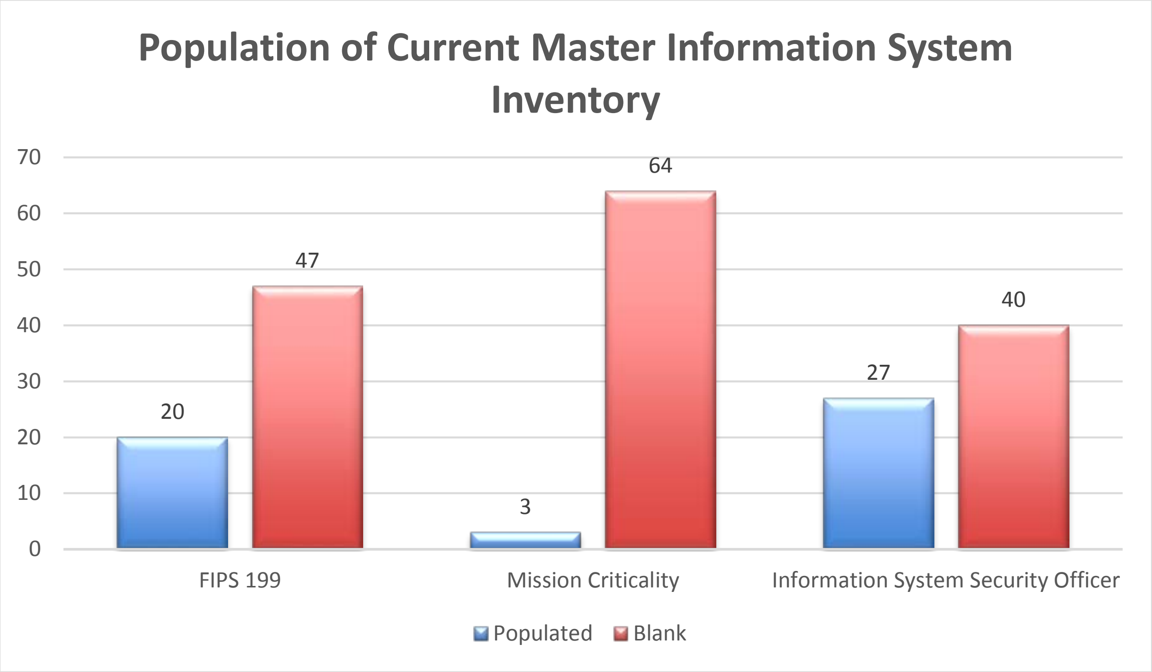
Information Services does not maintain a comprehensive and accurate information system inventory. We found missing data fields, inaccurate information, and information systems managed by NARA personnel and contractors that were not included on its master systems inventory. This occurred because Information Services has not finalized and implemented systems inventory guidance; has not documented a process for identifying information systems that should be listed on the inventory; and has not clearly defined who within Information Services is responsible for maintaining the information system inventory. 44 U.S.C. § 3505(c)[3] states the head of each agency shall develop and maintain an inventory of the information systems (including national security systems) operated by or under the control of such agency. Without comprehensive and accurate systems inventory, NARA has reduced assurance information systems are adequately acquired/engineered, operated, and maintained to provide acceptable security.

Incomplete Information

Approximately two thirds of the fields in NARA's master system inventory were blank (See Chart 1). For example, 47 out of the 67 systems on the inventory do not have a FIPS 199 categorization designated. In addition 64 systems do not have the Mission Criticality Designation documented. Finally, 40 out of 67 systems do not have an Information System Security Officer (ISSO) documented on the inventory. Without this information NARA did not have the quality information necessary to provide oversight of their information systems. The GAO Standards define quality information as appropriate, current, complete, accurate, accessible, and provided on a timely basis. Without security related information such as a FIPS 199 categorization or the ISSO documented, NARA has reduced assurance they are able to apply the appropriate security controls to NARA information systems.

[3] Please see footnote 2, there are two paragraph (c)s in 44 U.S.C. § 3505.

Chart 1: This chart is a depiction of the information populated in NARA master information system inventory.



Inaccurate Information

NARA's master information system inventory documented inaccurate information. For example, the master information system inventory documents NARA's network (NARANet) as having a low FIPS 199 categorization level. However, Information Services response to the OIG's survey documents NARANet as having a moderate FIPS 199 categorization level. In another example, the wrong system owner was listed for 3 out of the 4 Archival Preservation Systems (APS) on the inventory when all 4 APS systems should have had the same information system owner. Without quality information, Information Services could not confidently make security decisions or provide the appropriate oversight of NARA's information systems based on the master information system inventory.

Missing Information Systems

NARA's master information system inventory did not include all of the information systems managed by NARA and its contractors. The results from the survey used to determine the potential universe of systems throughout the agency identified 142 systems compared to the only 67 system identified in the master system inventory maintained by Information Services.

While NARA has developed a draft FISMA Inventory Standard to ensure all IT systems across NARA are appropriately reported, tracked and secured in accordance with NARA security policies and procedure. However, not all information systems managed by NARA or its contractors would be listed in NARA's FISMA Inventory. The draft standard states some IT systems will not be listed on NARA's FISMA Inventory depending on the classification of the system and whether the system was included in a General Support System's Security Assessment & Authorization, meaning not all systems will be included.

Additionally, NARA has not clearly defined who is responsible for maintaining the information system inventory. NARA Directive 101 designates the approved organizational units within NARA and the functional statements of these units. However, NARA Directive 101 does not define who has responsibility for the information system inventory. Without a comprehensive and accurate systems inventory, NARA has reduced assurance they are providing appropriate oversight of their information systems.

Recommendations

We recommend the CIO

Recommendation 1: Develop, document, approve and implement a process for developing and maintaining the system inventory, in adherence to 44 U.S.C. § 3505(c).

Management Response

NARA concurs with this recommendation. Information Services will develop, implement and provide procedures for the maintenance and annual review of the system inventory, in accordance to OMB Circular A-130 (A-130) and in adherence to 44 U.S.C. § 3505(c).

Target Completion Date: May 1, 2017

OIG Analysis

We consider NARA's proposed actions responsive to our report recommendations. All recommendations will remain open and resolved, pending completion of the corrective actions identified above.

Recommendation 2: Ensure all of the systems managed by NARA and its contractors are included in the inventory.

Management Response

NARA concurs with this recommendation. Information Services will manage and provide an inventory of systems following the guidance and requirements for information systems inventories per A-130 and 44 U.S.C. § 3505(c), applied in alignment with NARA criteria for the definition of systems, applications, and tools established in Recommendation 1.

Target Completion Date: August 30, 2017

OIG Analysis

We consider NARA's proposed actions responsive to our report recommendations. All recommendations will remain open and resolved, pending completion of the corrective actions identified above.

Recommendation 3: Update the inventory annually to ensure the information populated in the inventory is complete and accurate.

Management Response

NARA concurs with this recommendation. Information Services will document and provide the process for complete annual updates of the system inventory in the procedural document developed in Recommendation 1 and provide evidence of an annual.

Target Completion Date: May 1, 2017

OIG Analysis

We consider NARA's proposed actions responsive to our report recommendations. All recommendations will remain open and resolved, pending completion of the corrective actions identified above.

Recommendation 4: Document in NARA Directive 101 the organization responsible for maintaining the system inventory.

Management Response

NARA concurs with this recommendation. Information Services will ensure that NARA policy clearly identifies the organization responsible for maintaining and reviewing the annual system inventory. Information Services will provide a copy of the policy that assigns responsibility for maintaining the system inventory.

Target Completion Date: August 31, 2017

OIG Analysis

We consider NARA's proposed actions responsive to our report recommendations. All recommendations will remain open and resolved, pending completion of the corrective actions identified above.

Finding 2. Inaccurate FIPS 199 Categorizations

NARA system owners were not always adequately categorizing information systems using FIPS 199. Controls were not in place to ensure System owners used proper documentation to categorize the systems. System owners were either using incomplete FIPS 199 categorization documentation provided by Information Services or not using FIPS 199 at all to categorize their information system. According to NIST SP 800-60 Volume I, an incorrect FIPS 199 security categorization can result in the agency either over protecting the information system thus wasting valuable security resources, or under protecting the information system and placing important operations and assets at risk. Consequently, NARA may not be 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.

FIPS 199 is the standard used by all federal agencies to categorize all information and information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels assessed. A FIPS 199 categorization is the basis used to apply the appropriate NIST SP 800-53 version 4 security controls. In order to meet the FIPS 199 requirement, NARA developed a FIPS 199 assessment matrix that guides system owners in assigning information types and categorization levels to information in a system. However, the matrix did not include all of the information types listed in NIST SP 800-60 Volume II. According to FIPS 199, security categories for all information types resident on a system must be considered when categorizing an information system.

As previously indicated, we requested survey respondents to provide us with a list of information systems they are responsible for as well as the FIPS 199 categorization for each information system. Most of the survey responses included the FIPS 199 categorization level for their systems. We followed up with some respondents who provided us with FIPS 199 categorizations asking how they determined the categorization for the system. These respondents indicated using their best judgment to determine the FIPS 199 categorization for the system.

Recommendations

We recommend the CIO

Recommendation 5: Comply with FIPS 199 and NIST SP 800-60 to ensure all information systems are categorized.

Management Response

NARA concurs with this recommendation. Specifically, Information Services will comply with FIPS 199 and NIST SP 800-60 by ensuring all. NARA information systems are categorized and provide the systems inventory developed for Recommendation 2 as evidence of categorization.

Target Completion Date: September 30, 2017

OIG Analysis

We consider NARA's proposed actions responsive to our report recommendations. All recommendations will remain open and resolved, pending completion of the corrective actions identified above.

Recommendation 6: Comply with FIPS 199 and NIST SP 800-60 to ensure the categorization of information systems is accurate.

Management Response

NARA concurs with this recommendation. Specifically, Information Services will comply with FIPS 199 and NIST SP 800-60 by ensuring all. NARA information systems are categorized and provide the systems inventory developed for Recommendation 2 as evidence of categorization.

Target Completion Date: September 30, 2017

OIG Analysis

We consider NARA's proposed actions responsive to our report recommendations. All recommendations will remain open and resolved, pending completion of the corrective actions identified above.

Recommendation 7: Update the FIPS 199 guidance to include all information types listed in NIST SP 800-60 Volume II.

Management Response

NARA concurs with this recommendation. Specifically, Information Services will update the FIPS199_Assessment_Matrix_v.1.0 spreadsheet to reflect all information types listed in NIST SP 800-60 Volume II, Tables C-2 & D-2.

Target Completion Date: December 30, 2016

OIG Analysis

We consider NARA's proposed actions responsive to our report recommendations. All recommendations will remain open and resolved, pending completion of the corrective actions identified above.

Recommendation 8: Coordinate with system owners on validating their current FIPS 199 to ensure the systems categorization level is accurate.

Management Response

NARA concurs with this recommendation. Specifically, Information Services will validate with the system owner the categorizations of NARA systems on the inventory provided in Recommendation 2 and provide evidence of coordination.

Target Completion Date: September 30, 2017

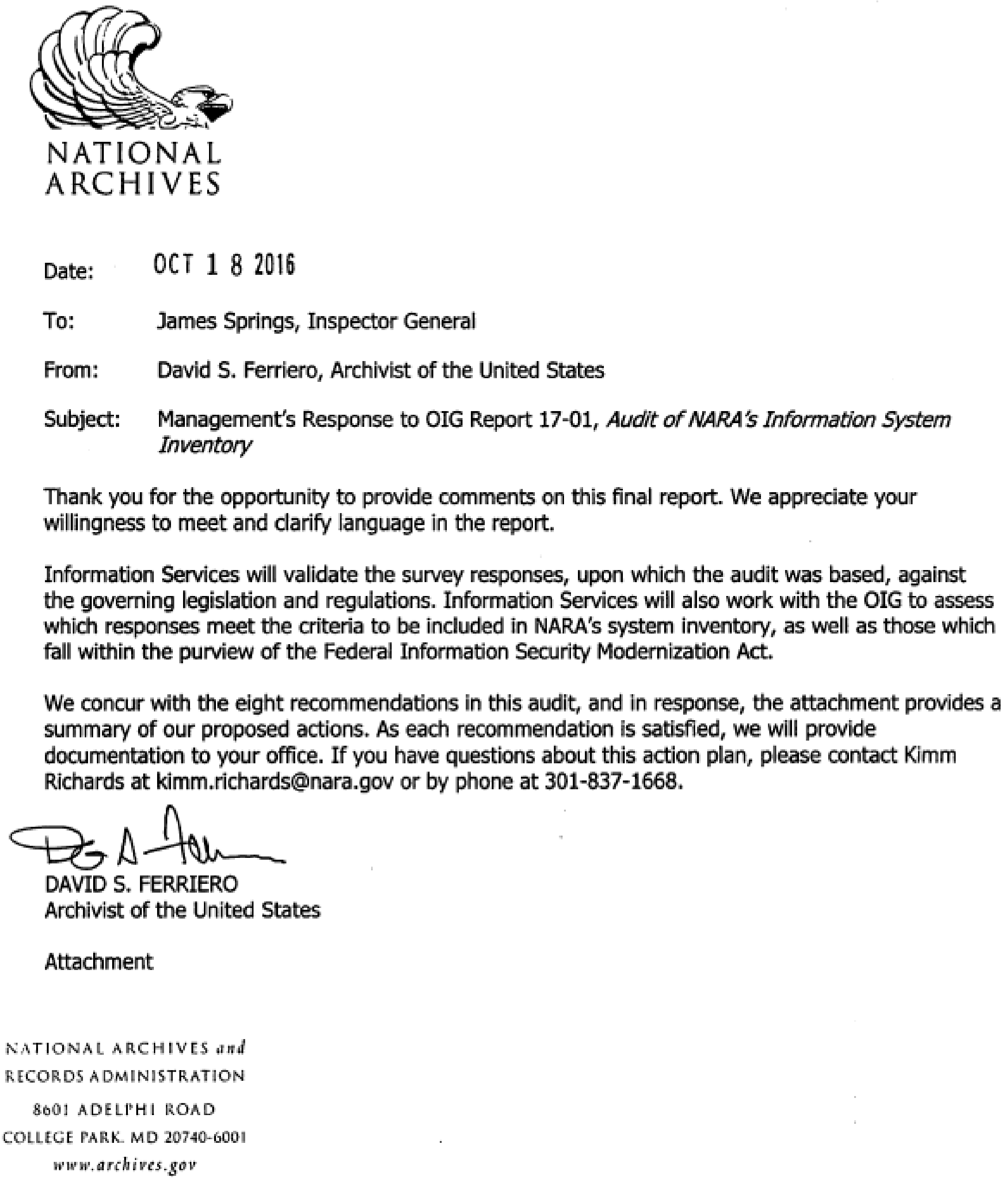
OIG Analysis

We consider NARA's proposed actions responsive to our report recommendations. All recommendations will remain open and resolved, pending completion of the corrective actions identified above.

Appendix A – Acronyms

APS	Archival Preservation System
CIO	Chief Information Officer
CPIC	Capital Planning and Investment Control
FISMA	Federal Information Security Modernization Act
FIPS 199	Federal Information Processing Standards Publication 199
GAO Standards	Government Accountability Office “Standards for Internal Control in the Federal Government”
GSS	General Support System
ISSO	Information System Security Officer
IT	Information Technology
NARA	National Archives and Records Administration
NARANet	NARA Network
NIST	National Institute of Standards and Technology
NIST SP	NIST Special Publication
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
U.S.C.	United States Code

Appendix B – Management Response



NATIONAL
ARCHIVES

Date: OCT 1 8 2016

To: James Springs, Inspector General

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

Subject: Management's Response to OIG Report 17-01, *Audit of NARA's Information System Inventory*

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

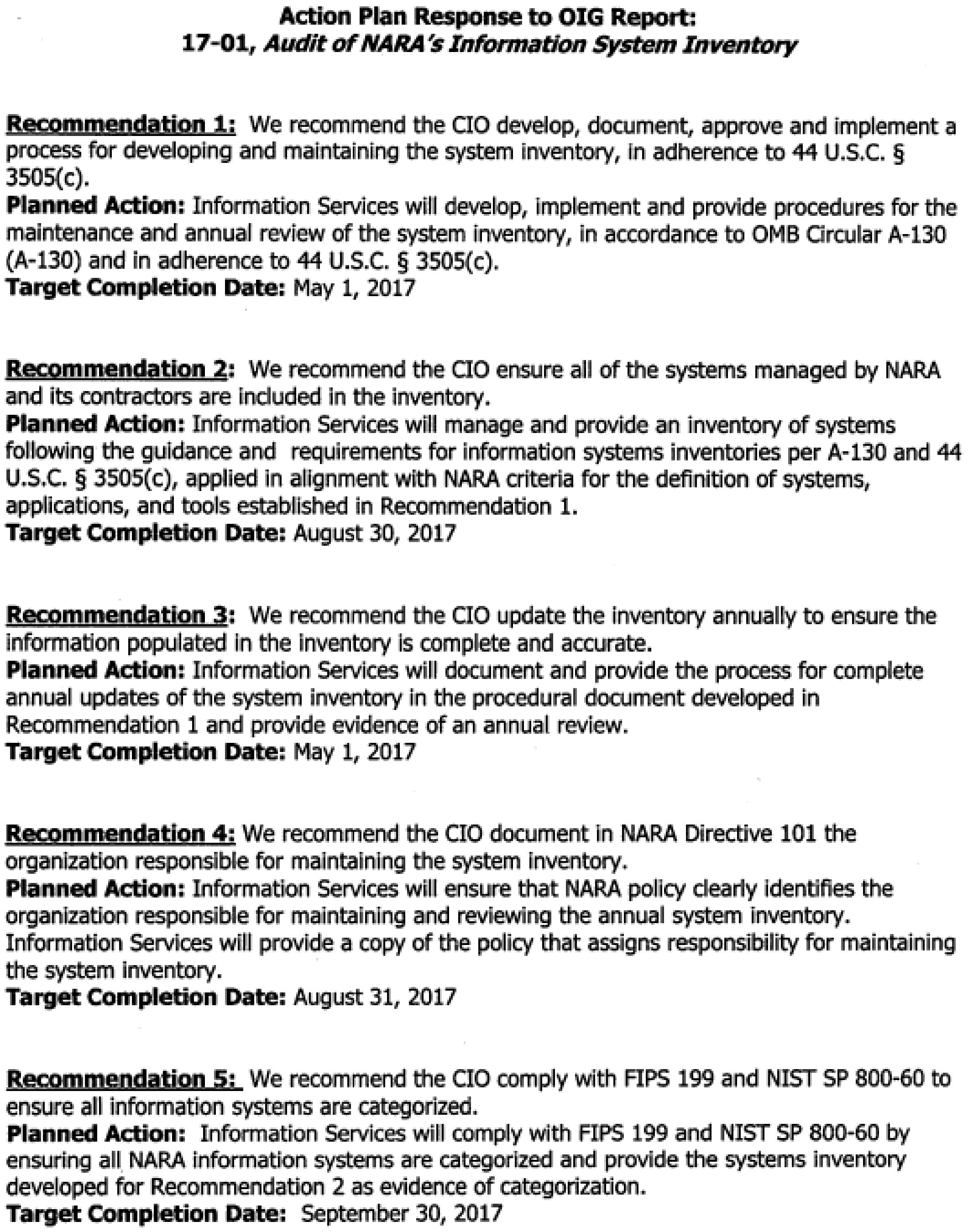
Information Services will validate the survey responses, upon which the audit was based, against the governing legislation and regulations. Information Services will also work with the OIG to assess which responses meet the criteria to be included in NARA's system inventory, as well as those which fall within the purview of the Federal Information Security Modernization Act.

We concur with the eight recommendations in this audit, and in response, the attachment provides a summary of our proposed actions. As each recommendation is satisfied, we will provide documentation to your office. If you have questions about this action plan, please contact Kimm Richards at kimm.richards@nara.gov or by phone at 301-837-1668.

DAVID S. FERRIERO
Archivist of the United States

Attachment

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



Action Plan Response to OIG Report:
17-01, *Audit of NARA's Information System Inventory*

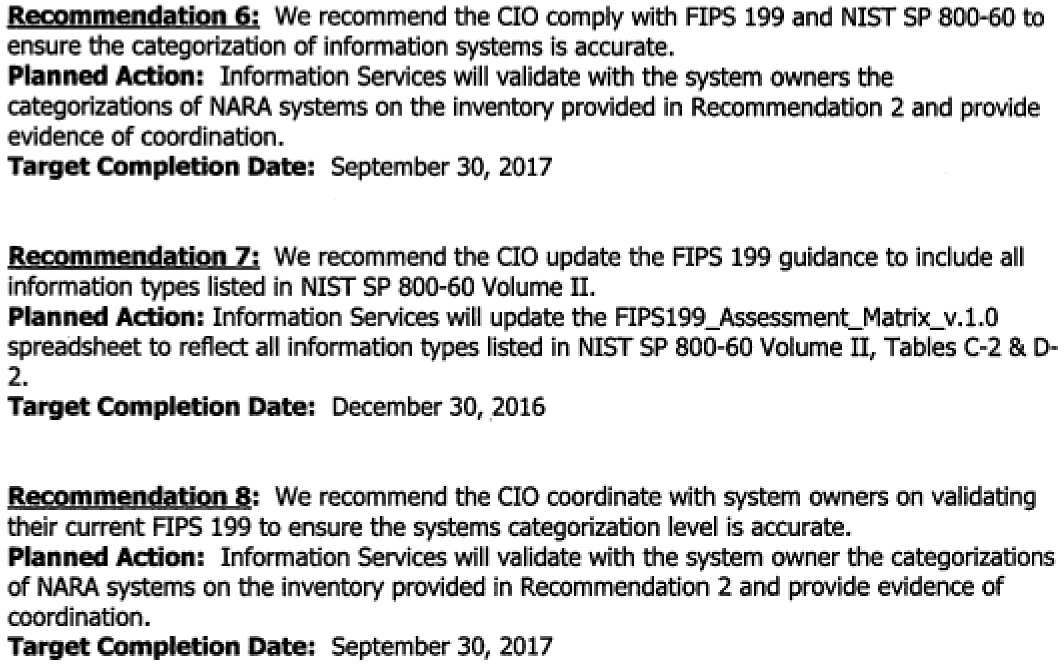
Recommendation 1: We recommend the CIO develop, document, approve and implement a process for developing and maintaining the system inventory, in adherence to 44 U.S.C. § 3505(c).
Planned Action: Information Services will develop, implement and provide procedures for the maintenance and annual review of the system inventory, in accordance to OMB Circular A-130 (A-130) and in adherence to 44 U.S.C. § 3505(c).
Target Completion Date: May 1, 2017

Recommendation 2: We recommend the CIO ensure all of the systems managed by NARA and its contractors are included in the inventory.
Planned Action: Information Services will manage and provide an inventory of systems following the guidance and requirements for information systems inventories per A-130 and 44 U.S.C. § 3505(c), applied in alignment with NARA criteria for the definition of systems, applications, and tools established in Recommendation 1.
Target Completion Date: August 30, 2017

Recommendation 3: We recommend the CIO update the inventory annually to ensure the information populated in the inventory is complete and accurate.
Planned Action: Information Services will document and provide the process for complete annual updates of the system inventory in the procedural document developed in Recommendation 1 and provide evidence of an annual review.
Target Completion Date: May 1, 2017

Recommendation 4: We recommend the CIO document in NARA Directive 101 the organization responsible for maintaining the system inventory.
Planned Action: Information Services will ensure that NARA policy clearly identifies the organization responsible for maintaining and reviewing the annual system inventory. Information Services will provide a copy of the policy that assigns responsibility for maintaining the system inventory.
Target Completion Date: August 31, 2017

Recommendation 5: We recommend the CIO comply with FIPS 199 and NIST SP 800-60 to ensure all information systems are categorized.
Planned Action: Information Services will comply with FIPS 199 and NIST SP 800-60 by ensuring all NARA information systems are categorized and provide the systems inventory developed for Recommendation 2 as evidence of categorization.
Target Completion Date: September 30, 2017



Recommendation 6: We recommend the CIO comply with FIPS 199 and NIST SP 800-60 to ensure the categorization of information systems is accurate.
Planned Action: Information Services will validate with the system owners the categorizations of NARA systems on the inventory provided in Recommendation 2 and provide evidence of coordination.
Target Completion Date: September 30, 2017

Recommendation 7: We recommend the CIO update the FIPS 199 guidance to include all information types listed in NIST SP 800-60 Volume II.
Planned Action: Information Services will update the FIPS199_Assessment_Matrix_v.1.0 spreadsheet to reflect all information types listed in NIST SP 800-60 Volume II, Tables C-2 & D-2.
Target Completion Date: December 30, 2016

Recommendation 8: We recommend the CIO coordinate with system owners on validating their current FIPS 199 to ensure the systems categorization level is accurate.
Planned Action: Information Services will validate with the system owner the categorizations of NARA systems on the inventory provided in Recommendation 2 and provide evidence of coordination.
Target Completion Date: September 30, 2017

Appendix C – Report Distribution List

Archivist of the United States
Deputy Archivist of the United States
Chief Operating Officer
Deputy Chief Operating Officer
Chief of Management and Administration
Executive for Information Services/Chief Information Officer
Deputy Chief Information Officer
Accountability

OIG Hotline

To report fraud, waste, or abuse, please contact us:

Electronically: https://www.archives.gov/oig/referral-form/index.html

Telephone: 301-837-3500 (Washington, D.C. Metro Area)
1-800-786-2551 (toll-free and outside the Washington, D.C. metro area)

Mail: IG Hotline
NARA
P.O. Box 1821
Hyattsville, MD 20788-0821