OFFICE of INSPECTOR GENERAL
NATIONAL ARCHIVES

February 12, 2020

TO: David S. Ferriero
               Archivist of the United States

FROM: James Springs
               Inspector General

SUBJECT: *Compendium of Open OIG Recommendations to NARA*
               OIG Special Report No. 20-R-04

The National Archives and Records Administration (NARA) Office of Inspector General (OIG) is charged with detecting and preventing fraud, waste, mismanagement, and abuse of agency programs and operations. The OIG makes recommendations designed to promote economy, efficiency, and effectiveness of NARA. The purpose of this Special Report is to summarize NARA OIG's recommendations that remain open as of September 30, 2019. An open recommendation is a recommendation previously documented in a report for which agreed upon corrective actions have not been implemented by NARA.

Tracking OIG Recommendations

The Office of Management and Budget Circular A-50 Revised, *Audit Followup*, indicates Audit followup is an integral part of good management, and is a shared responsibility of agency management officials and auditors. Requirements include (1) agencies shall assign a high priority to the resolution of audit recommendations and to corrective action and (2) resolution shall be made within a maximum of six months after issuance of a final report. Timely resolution and closure of open recommendations is imperative as NARA's future annual budget justifications to Congress, must include (1) a report listing each recommendation for corrective action from the OIG and (2) a report on the implementation status of each recommendation in accordance with the 2019 Good Accounting Obligation in Government Act.

NARA Management and the OIG share the responsibility to followup on recommendations. NARA Management is responsible for implementing recommendations promptly. The OIG is responsible for assessing NARA's implementation of corrective action and determining whether the action taken met the intent of the recommendation. NARA and the OIG have worked cooperatively to ensure our recommendations, and their corrective actions meet the intent of the recommendations.

Status of Open Recommendations

As of September 30, 2019, NARA closed 114 of 346 total open recommendations identified at the beginning of FY 2019. However, it continues to be apparent the importance of closing open

recommendations still varies among offices. Although NARA offices were given the opportunity to revise implementation dates in FY 2018, majority of the offices exceeded their revised implementation dates and did not provide documentation supporting actions taken to support closure of the recommendations.

Based on the documentation received, the Office of the Chief Financial Officer (CFO) has not made closing open recommendations a priority. In FY 2019, the CFO Office subsumed one and closed three open recommendations. As of September 30, 2019, the CFO Office still had 28 open recommendations resulting from audits conducted between FY 2013 through FY 2019. Since issuance of the associated audit reports, the CFO Office has not provided any documentation to the OIG in an effort to close 20 of these recommendations although revised implementation dates were granted in FY 2018. There has also been no communication with the OIG in addressing these open recommendations, many of which pointed to internal controls. Without maintainable action plan dates NARA will continue to face a mounting list of open recommendations that are well beyond the years when they were first identified. Additionally, without implementation of the recommendations, NARA continues to lack internal controls in many of its program areas.

The attachment provides a summary of our review of the open recommendations (Figures 1 through 3), including a detailed listing of all open recommendations (see pages 8-58). The OIG continues to report quarterly to NARA management on the agency's progress in closing recommendations.

The OIG will continue to meets its responsibilities as required for audit followup and looks forward to working with NARA Management in their efforts to implement corrective actions that will help reduce the number of open recommendations.

As with all OIG products, we determine what information is publically posted on our website from the attached 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.

Attachment

cc: Debra Wall, Deputy Archivist of the United States
       William Bosanko, Chief Operating Officer
       Chris Naylor, Deputy Chief Operating Officer
       Micah Cheatham, Chief of Management and Administration
       Valorie, Findlater, Acting Chief Human Capital Officer
       Swarnali Haldar, Chief Information Officer

Colleen Murphy, Chief Financial Officer
Pamela Wright, Chief Innovation Officer
Gary Stern, General Counsel
Laurence Brewer, Chief Records Officer
Oliver Potts, Director of Federal Register
Jay Trainer, Executive for Agency Services
Ann Cummings, Executive for Research Services
Susan Donius, Acting Executive for Legislative Archives, Presidential Libraries, and Museum Services
Donna Forbes, Executive for Business Support Services
Kimm Richards, Accountability
United States House Committee on Oversight and Government Reform
Senate Homeland Security and Governmental Affairs Committee

Summary of Open Recommendations

This report identifies 293 open recommendations from OIG reports as of September 30, 2019. Majority of the open recommendations are within Information Services (see Figure 1). It also includes three recommendations that remain unresolved because NARA has not agreed to implement the recommendations or provided proposed actions to resolve the deficiencies identified in audit reports.

Figure 1. Number of Open Recommendations by Office as of September 30, 2019

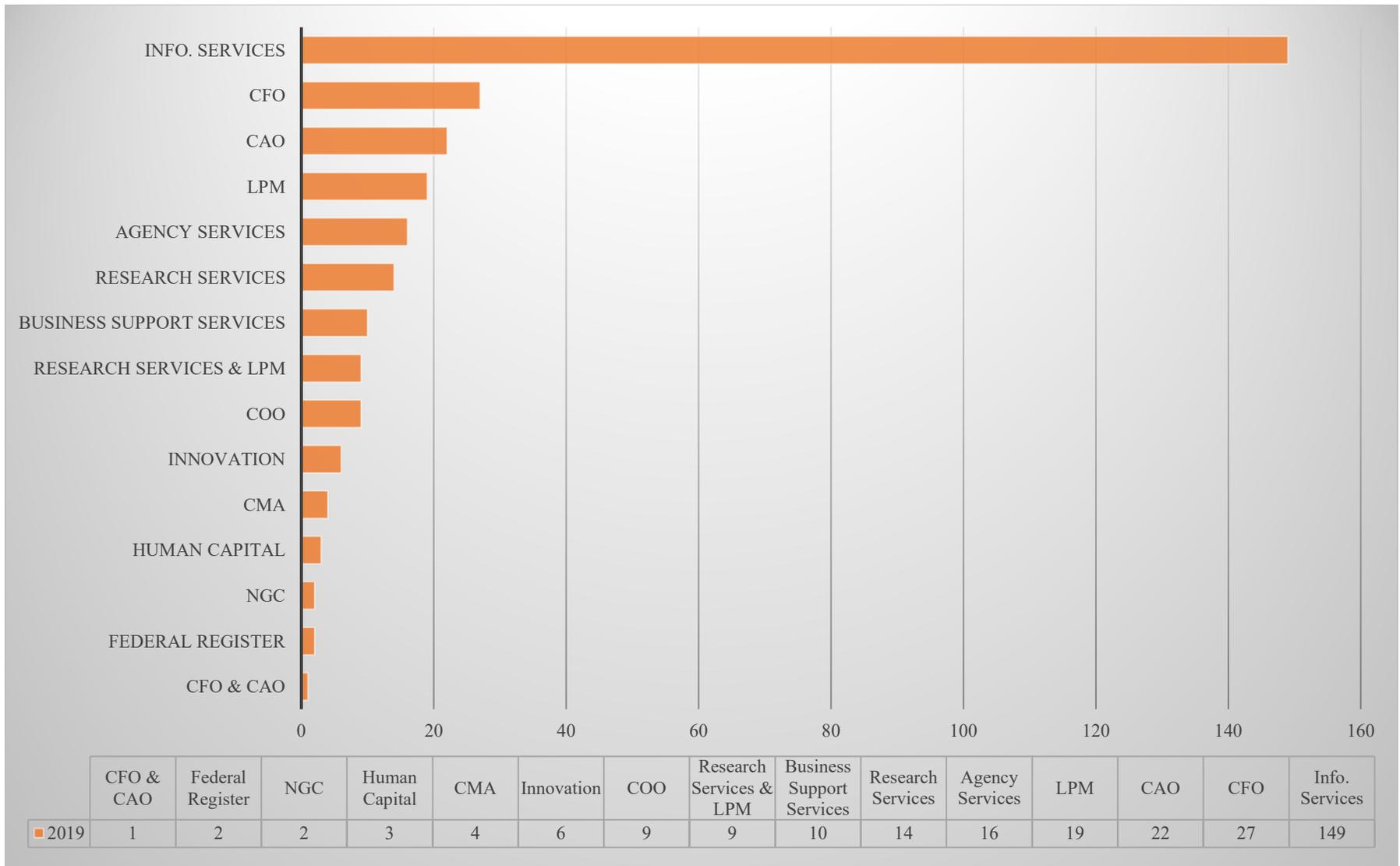|	CFO & CAO	Federal Register	NGC	Human Capital	CMA	Innovation	COO	Research Services & LPM	Business Support Services	Research Services	Agency Services	LPM	CAO	CFO	Info. Services
2019	1	2	2	3	4	6	9	9	10	14	16	19	22	27	149

Figure 2 summarizes the number of recommendations opened and closed by NARA OIG since September 30, 2019.

Figure 2. Number of Open Recommendations as of September 30, 2019
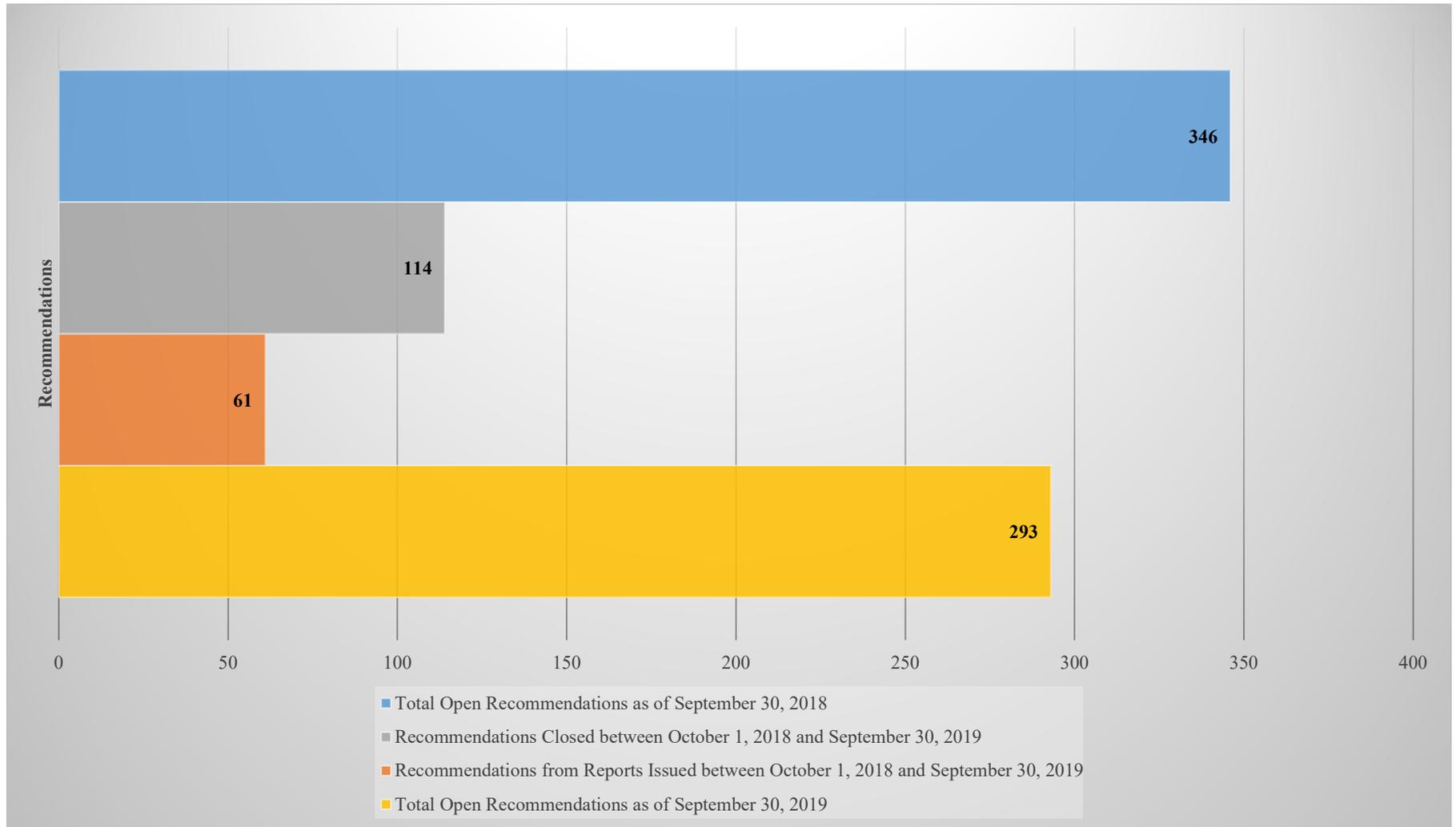
As of September 30, 2019, there were 243 open recommendations with implementation dates aging between less than one to six years old (see Figure 3).

Figure 3. Number of Open Recommendations as of September 30, 2019
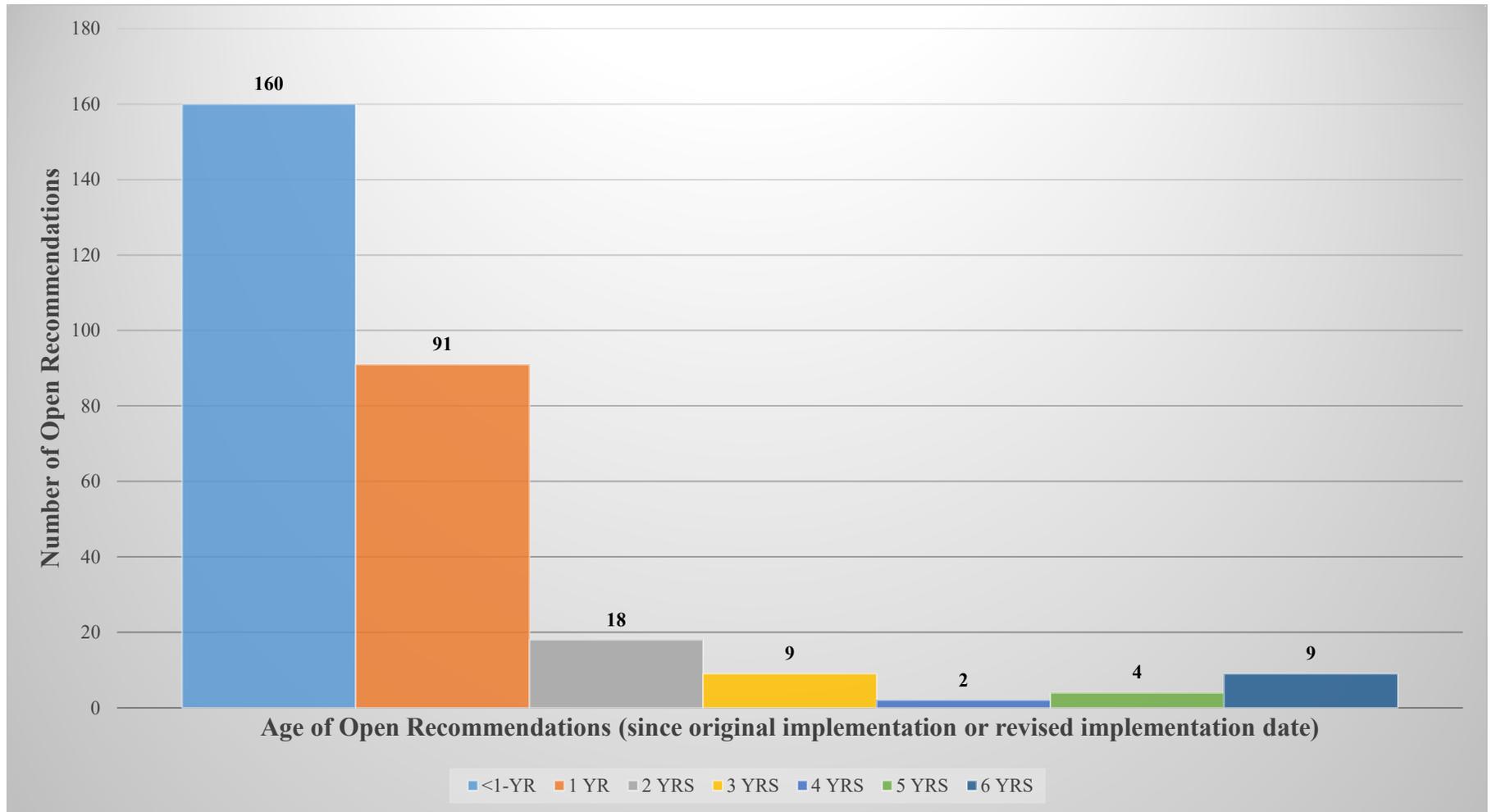
Open Recommendations as of September 30, 2019

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
	Audit of NARA's Work at Home System (09-15)					
7	The CIO ensures that the WAHS meets OMB and NIST requirements prior to full implementation.	Information Services	9/29/2009	6/1/2010	0	9/30/2019
	Audit of NARA's Oversight of Electronic Records Management in the Federal Government (10-04)					
5	The Assistant Archivist for Records Services, Washington DC (NW) should ensure development of controls to adequately monitor agency scheduling of electronic records in an effort to reasonably ensure electronic records/systems are scheduled in timely manner, and therefore provide a reasonably accurate reflection of the universe of electronic records.	Agency Services	4/2/2010	12/31/2016	0	9/30/2019
	Network and Penetration Testing Oversight (11-02)					
2b	This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.	Information Services	11/8/2010	2/28/2011	273	12/31/2018
3c	This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.	Information Services	11/8/2010	3/21/2011	304	11/30/2018

---

[1]Calculated based on the latest of either the original implementation or revised implementation date (if applicable).

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
6a	NARA management should immediately address corrective action for all vulnerabilities identified as "high" and "critical" risk.	Information Services	11/8/2010	3/31/2011	61	7/31/2019
6b	NARA Management should evaluate the identified risks and corrective actions to address those identified as "medium" and "low" risk vulnerabilities.	Information Services	11/8/2010	6/15/2011	61	7/31/2019
Audit of NARA's Data Center Consolidation Initiative (12-09)						
1b	The CIO should update the Master System List and/or Enterprise Architecture to incorporate energy usage calculations.	Information Services	5/10/2012	8/31/2012	273	12/31/2018
1c	The CIO should update the Master System List and/or the Enterprise Architecture to incorporate realistic estimates of funding needed or savings to be realized from implementing NARA's data center consolidation goals.	Information Services	5/10/2012	11/30/2012	273	12/31/2018
1d	The CIO should update the Master System List and/or the Enterprise Architecture to incorporate annual savings metrics such as rack count reduction, server count reduction, energy usage reduction, and energy cost reduction to monitor progress.	Information Services	5/10/2012	11/30/2012	273	12/31/2018
3	The CIO should conduct the consolidation/virtualization analysis to investigate the impact of consolidating or virtualizing two major application domains (NISP and ERA) and the General Support System (NARANET) as planned, or evaluate other alternatives to increase the average server utilization rate.	Information Services	5/10/2012	11/30/2012	273	12/31/2018
4	The Executive for Business Support Services should evaluate the current organization of rack space and	Information Services	5/10/2012	11/30/2012	273	12/31/2018

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
	determine whether servers can be consolidated into fewer racks when considering space optimization, power consumption, operations management, and component failure/recovery perspectives.					
Follow-up on OIG Audit Report 08-01: Audit of the Process of Safeguarding and Accounting for Presidential Library Artifacts (12-10)					
2b	Review and revise current time-guidance policy, as appropriate, for baseline inventories for newly established Presidential libraries.	LPM	9/13/2012	12/31/2013	365	9/30/2018
7a	Policies and procedures are clarified and reiterated to library personnel concerning 1) sequestration of museum artifacts from library personnel other than museum personnel, and 2) procedures to periodically review access logs and security camera tapes.	LPM	9/13/2012	12/31/2013	365	9/30/2018
7b	Policies and procedures for artifacts on long-term loan are re-iterated and disseminated concerning 1) the annual update of loan agreements and 2) requirements for long-term loans including photo requirements. LP should establish time caps on loans or periodically request temporary return of items for condition assessments.	LPM	9/13/2012	5/24/2013	92	6/30/2019
8a	Update comprehensive set of museum collection management policies and procedures and ensure their development.	LPM	9/13/2012	12/31/2014	273	12/31/2018
8b	Establish procedures to periodically review and, if necessary, revise said policies and procedures.	LPM	9/13/2012	12/31/2014	92	6/30/2019
NARANet Network Assessment Oversight (12-11)					

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
14	This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.	Information Services	8/27/2012	2/28/2014	0	9/30/2019
20	This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.	Information Services	8/27/2012	11/30/2013	2130	No Change
35	This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.	Information Services	8/27/2012	12/15/2013	0	9/30/2019
48	This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information. *Unresolved - The agency did not agree to implement the recommendation.*	Information Services	8/27/2012	Unresolved	N/A	N/A
Audit of NARA's Classified Systems (12-15)						
1	The Executive for Information Services/CIO (I), in coordination with the Chief Operating Officer (C), should ensure all classified system authorization packages are updated in accordance with NARA policy.	Information Services	7/23/2012	1/31/2013	273	12/31/2018
2	I, in coordination with C, should establish a timeframe for review and approval of authorization documents.	Information Services	7/23/2012	1/31/2013	273	12/31/2018

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
3	I, in coordination with C, should develop a continuous monitoring strategy for classified systems requiring system owners on at least a quarterly basis to assess security controls and inform authorizing officials when changes occur that may impact the security of the system.	Information Services	7/23/2012	1/31/2013	273	12/31/2018
4	I, in coordination with C, should obtain authorizations to operate for each of the classified systems or disallow them in accordance with NARA and Federal policy.	Information Services	7/23/2012	1/31/2013	273	12/31/2018
Audit of NARA's Internal Control Program (13-01)						
1e	Risk management responsibilities are included in the performance plans for program and function owners.	CFO	12/10/2012	9/30/2013	2191	No Change
Audit of NARA's Preservation Program (13-08)						
1a	The Archivist should ensure an overarching preservation strategy is developed. Additionally, a risk-based approach to holistically assess the agency's preservation needs and design the agency's preservation plan should be implemented.	Research Services	7/9/2013	6/30/2014	61	7/31/2019
1b	The Archivist should ensure an analysis is conducted of the organizational structure and responsibilities of each office involved in preservation. This should include a determination whether the preservation strategy can be effectively implemented with a decentralized structure, or if one NARA office should have authority over the entire Preservation Program.	Research Services	7/9/2013	3/31/2014	61	7/31/2019
2	The Chief Innovation Officer and Executives for Research Services and Legislative Archives, Presidential Libraries and Museum Services, should ensure	Research Services	7/9/2013	6/30/2014	61	7/31/2019

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
	comprehensive preservation policies and procedures for each of their organizations are developed and/or updated.					
3a	The Chief Innovation Officer and Executives for Research Services and Legislative Archives, Presidential Libraries and Museum Services should completely identify the resources necessary to adequately accomplish NARA's preservation mission.	Research Services	7/9/2013	6/30/2014	-92	12/31/2019
3b	Develop a plan to identify the complete universe of textual and non-textual records that require preservation.	Research Services	7/9/2013	3/31/2014	-92	12/31/2019
4	The Executive for Research Services should ensure a detailed analysis is performed and communicate about the risks versus the benefits associated with not using the existing risk assessment data to calculate the backlog for the Washington area Archives.	Research Services	7/9/2013	11/29/2013	-92	12/31/2019
5a	The Executive for Research Services should ensure an analysis is performed to determine if additional risk assessments for the Washington area Archives and Presidential Libraries including older holdings should be completed. Identify the risks for not completing the assessments.	Research Services	7/9/2013	11/29/2013	-92	12/31/2019
5b	The Executive for Research Service should ensure additional measurable performance metrics are developed and implemented to track the progress within the Preservation Program.	Research Services	7/9/2013	6/30/2014	61	7/31/2019

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
5c	The Executive for Research Services should ensure a cost benefit analysis for the HMS circulation Module is completed. Request required resources if the cost benefit analysis identifies benefits to the agency.	Research Services	7/9/2013	3/31/2014	2009	No Change
6	The Executive for Legislative Archives, Presidential Libraries and Museum Services should ensure an analysis is performed to identify whether HMS should be implemented across the Libraries. If it is decided HMS will be implemented, a timeline should be established. If it is decided HMS will not be implemented, identify (1) how the existing system will meet the agency's preservation needs and (2) obstacles and risks for not implementing HMS.	LPM	7/9/2013	11/29/2013	2131	No Change
Audit of NARA's Preservation Program (13-10)						
1a	The COO should ensure a comprehensive review of the Standards is completed. Additionally, roles and responsibilities for offices involved in the execution of the directive are clearly defined.	Research Services	7/9/2013	12/31/2013	2099	No Change
1b	The COO should ensure a plan is developed including a timeline for when the archival storage facility reviews will be completed.	COO	7/9/2013	3/31/2014	2009	No Change
1c	The COO should ensure an accurate listing of facilities currently compliant with the Standards along with the area of deficiencies is identified and communicated.	COO	7/9/2013	3/31/2014	2009	No Change
1d	The COO should ensure resources needed to make all archival storage facilities compliant by 2016 are identified. If the facility cannot be brought into conformance with the Standards, determine and	COO	7/9/2013	12/31/2013	2099	No Change

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
	document what mitigating actions have been implemented.					
1e	The COO ensures Performance Measurement and Reporting System (PMRS) is updated to accurately reflect percentage of archival holdings in appropriate space.	COO	7/9/2013	12/31/2013	2099	No Change
	Audit of the ERA System's Ability to Ingest Records (13-11)					
1	The COO assess Federal agency usage of Base ERA and implement a process to improve the records management workload and records management practices that exist between NARA and Federal agencies to ensure electronic records are being properly transferred into Base ERA.	Agency Services	9/19/2013	12/31/2014	1734	No Change
2	The COO identify the most efficient and effective method of ingest and require Federal agencies to follow this method when transferring electronic records into base ERA. In addition this information should be properly disseminated to Federal agencies.	Research Services	9/19/2013	12/31/2014	1734	No Change
	Audit of NARA's Processing of Textual Records (13-14)					
5a	The Executive for Legislative Archives, Presidential Libraries and Museums should work with the Performance and Accountability Office to develop a performance measure for tracking the process of electronic presidential records.	LPM	9/18/2013	12/31/2014	1734	No Change
5b	Determine the true backlog of electronic presidential records and determine if additional resources are needed and can be obtained to handle the increased workload.	LPM	9/18/2013	3/31/2015	1644	No Change

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
Audit of Select Aspects of NARA's Sustainability Program: Energy Savings Performance Contracts (14-01)
8	NARA should establish formal assessment criteria and future savings analysis for use in determining whether to cancel ESPCs.	CFO	1/30/2014	9/30/2015	183	3/31/2019
Audit of NARA's CPIC Process (14-08)
1b	The CIO should ensure all required CPIC related documentation is completed for all NARA IT investments going through the CPIC process.	Information Services	4/17/2014	2/27/2015	94	6/28/2019
1c	The CIO should require the creation and use of a checklist outlining the IT governance related documentation required to be completed for all IT investments going through the CPIC process.	Information Services	4/17/2014	6/30/2015	273	12/31/2018
2	The CIO should require NARA's updated CPIC policies and procedures meet the CPIC process requirements detailed in the Clinger Cohen Act.	Information Services	4/17/2014	6/30/2015	273	12/31/2018
3	The Chief Operating Officer (COO) should ensure NARA IT investments do not bypass NARA's CPIC process.	Information Services	4/17/2014	6/30/2015	1553	No Change
5	The COO should ensure I-P maintains documentation of its approval of IT investments in PRISM and I-P's PRISM approval of IT investments is tested on an annual basis with all documentation of this testing sent to NARA's internal controls group.	Information Services	4/17/2014	8/31/2015	273	12/31/2018
6	The COO should ensure the training guide for purchase card holders is updated to include a discussion of the requirements of NARA's CPIC Process.	CAO	4/17/2014	8/31/2015	1491	No Change

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
8	The CIO should ensure NARA's IT governance process, which includes CPIC, incorporates the lessons learned when Directive 801 was followed to create a more user-friendly, streamlined, and transparent policy where CPIC requirements align closely with the costs of IT investments.	Information Services	4/17/2014	6/30/2015	183	12/31/2018
Oversight of the Audit of Enterprise Wireless Access (14-10)						
1e	NARA should authorize network operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the nation resulting from the operation of the information system and the decision that this risk is acceptable.	Information Services	5/9/2014	12/31/2014	183	3/31/2019
4a	NARA should utilize existing WLC and WAP baseline configurations or develop its own baseline configurations.	Information Services	5/9/2014	10/29/2014	183	7/31/2019
4b	NARA should implement a process to monitor the WLC and WAP settings for compliance with the established baseline configurations.	Information Services	5/9/2014	10/29/2014	61	7/31/2019
4c	NARA should document and approve any deviations from the WLC and WAP baseline configurations.	Information Services	5/9/2014	10/29/2014	61	7/31/2019
4d	NARA should maintain older versions of the baseline configurations as necessary.	Information Services	5/9/2014	12/31/2014	61	7/31/2019
Audit of NARA's Mobile Device Management (15-02)						
1a	Develop and document a strong internal control process for ordering, activating, and deactivating mobile devices	Information Services	11/12/2014	4/30/2015	0	9/30/2019

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
	and phone lines to ensure no unnecessary phone lines exist and incur costs. *Funds Put to Better Use - $7,289*					
1b	Develop and document a strong internal control process for reviewing monthly bills for items including user names, activities, plan adequacy, and opportunity for cost savings.	Information Services	11/12/2014	4/30/2015	0	9/30/2019
1c	Develop and document a strong internal control process for determining when an additional charge will be considered for reimbursement. *Funds Put to Better Use - $2,745*	Information Services	11/12/2014	4/30/2015	0	9/30/2019
2	Review and update NARA's current policy documents for use of NARA-issued mobile devices, including NARA 813-1 and NARA 802 to reflect more complete and accurate information an acceptable uses of the devices and when a disciplinary action will be requested.	Information Services	11/12/2014	4/30/2015	61	7/31/2019
3	Provide training to educate users on acceptable uses of NARA-issued mobile devices, including requesting a travel device for international travel.	Information Services	11/12/2014	8/31/2015	0	9/30/2019
4	Develop a formal policy for interaction of NARA-issued mobile devices with other systems and update NARA 813-1 to clearly reflect the policy.	Information Services	11/12/2014	4/30/2015	61	7/31/2019
Audit of Specially Protected Records (15-03)						

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
2a	Security Management performs initial certifications of Specially Protected Holdings (SPHs) storage areas.	COO	2/6/2015	7/31/2017	0	9/30/2019
2b	Security Management performs security inspections of SPHs storage areas.	COO	2/6/2015	7/31/2017	0	9/30/2019
2c	Security Management develops guidelines for SPHs security inspections, including timeframes, criteria, documenting requirements, and reporting requirements.	COO	2/6/2015	7/31/2017	0	9/30/2019
4	Ensure Security Management maintains copies or obtains access to SPHs inventory listings and use them to randomly select records and verify their condition and location during inspections.	COO	2/6/2015	7/31/2017	0	9/30/2019
5a	Ensure SPHs inventory listings are completed at the item level. Establish a timeframe for when the listings must be completed. Communicate with other offices to identify best practices used in documenting their inventories.	Research Services, LPM	2/6/2015	9/28/2018	183	Research Services - No Update LPM - 3/31/2019
5b	Ensure inventory listings are reviewed to determine their accuracy and update as necessary.	Research Services, LPM	2/6/2015	9/28/2018	183	Research Services - No Update LPM - 3/31/2019
5c	Ensure a finding aid is created for the agency's entire SPHs collection at the item level.	Research Services, LPM	2/6/2015	9/28/2018	183	Research Services - No Update

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
						LPM - 3/31/2019
5d	Ensure locked hard copies of the inventory listings are maintained.	Research Services, LPM	2/6/2015	9/28/2018	183	Research Services - No Update

LPM - 3/31/2019 |
| 5e | Ensure SPHs inventory listings are maintained in the Holdings Management System (HMS). Until HMS is implemented by all offices, ensure all electronic versions of the listings are password protected and access limited to authorized employees. | Research Services, LPM | 2/6/2015 | 9/28/2018 | 183 | Research Services - No Update

LPM - 3/31/2019 |
| 7 | Ensure all Presidential Libraries are in compliance with NARA 1572 policy of conducting annual inspections. | LPM | 2/6/2015 | 8/31/2017 | 30 | 8/31/2019 |
| 8a | Initial inspections of SPHs inventory are completed. | Research Services, LPM | 2/6/2015 | 8/31/2017 | 30 | Research Services - No Update

LPM - 8/31/2019 |
| 8b | Custodial units are in compliance with NARA 1572, including randomly inspecting at least 3% of SPHs inventory annually on a rotating basis and using one individual that does not work for the individual responsible for the inspection. | Research Services, LPM | 2/6/2015 | 8/31/2017 | 30 | Research Services - No Update

LPM - 8/31/2019 |

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
8c	Annual inspection reports include at a minimum date of inspection, individuals that complete the inspections, and a listing of items inspected, including their location and physical condition.	Research Services, LPM	2/6/2015	8/31/2017	30	Research Services - No Update LPM - 8/31/2019
8d	Annual inspection results are adequately documented and communicated to Security Management and office heads.	Research Services, LPM	2/6/2015	8/31/2017	30	Research Services - No Update LPM - 8/31/2019
9a	Staff is properly trained or retrained to use charge out cards whenever records are removed from SPHs storage areas.	LPM	2/6/2015	7/31/2017	365	9/30/2018
10a	Required elements for the handling of SPHs for each record storage area should be communicated to each custodial unit.	Research Services, LPM	2/6/2015	7/31/2017	61	7/31/2019
10b	Detailed procedures are documented for each custodial unit.	Research Services, LPM	2/6/2015	7/31/2017	60	8/1/2019
10c	A process is in place for periodic review of procedures and updates are made as needed.	Research Services, LPM	2/6/2015	7/31/2017	59	8/2/2019
	Audit of Digitization Storage (15-11)					
6	Develop a long-term strategy for increasing transfer capabilities between various internal storage systems housing digitized records.	Information Services	5/5/2015	12/31/2015	273	12/31/2018

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
	Audit of NARA's Human Resource (HR) Systems and Data Accuracy (15-13)					
1	Fully implement the new supervisor information update process in FPPS and conduct a review of the information on a periodic basis to ensure the information remains accurate and complete.	Human Capital	8/24/2015	7/31/2016	365	9/30/2018
10	Re-evaluate the option to utilize eCStaffing to manage personnel data for non-Federal workforce at NARA and use the HRMS as the single authoritative data source for the HSPD-12 LACS implementation.	Human Capital	8/24/2015	6/30/2016	1187	No Change
11	Establish on authoritative data source that provides the latest data to role-based users on NARA's Federal employees, contractors, and volunteers at the enterprise level.	Information Services	8/24/2015	9/30/2016	273	12/31/2018
	Audit of NARA's Space Management (15-14)					
3	Work with R to facilitate consistent application of HMS at all archival facilities, to capture all archival holdings in HMS, and improve how HMS calculates the available space.	Research Services	9/29/2015	10/31/2016	365	9/30/2018
	Oversight of NARA's Cable Infrastructure Assessment (15-15)					
1	NARA should incorporate all locations into the NARANet SA&A package by documenting location-specific security controls and ensuring that they are appropriately tested and monitored.	Information Services	9/30/2015	6/30/16	1187	No Change
2.1	Ensure that neat cable management and labeling mechanisms are employed for all sites.	Information Services	9/30/2015	8/31/2016	1125	No Change

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
2.2	Ensure that all server rooms are equipped with appropriate fire detection and suppression capabilities.	Business Support Services	9/30/2015	10/31/2016	184	3/30/2019
2.3	Limit access to all server rooms to those individuals with an explicit need to access IT equipment.	Business Support Services	9/30/2015	10/31/2016	184	3/30/2019
2.4	Ensure that appropriate temperature and humidity monitoring and control mechanisms are employed for all server rooms.	Business Support Services	9/30/2015	10/31/2016	184	3/30/2019
2.5	Ensure that appropriate UPS devices are employed for hardware supporting the site's network infrastructure.	Business Support Services	9/30/2015	10/31/2016	365	9/30/2018
2.6	Ensure that all server racks, switches, and network equipment are adequately secured from unauthorized access via locked racks.	Information Services	9/30/2015	4/26/2016	1252	No Change
3	NARA should develop and implement a plan to install additional networking capabilities at facilities that are near capacity, or develop and implement a contingency plan to support continued operations in the event that networking capabilities are maximized.	Information Services	9/30/2015	5/31/2016	1217	No Change
	Audit of NARA Web Hosting (16-01)					
1	The Chief Operating Officer (COO) should coordinate with the Chief Innovation Officer (CINO) to clearly define a business owner for the public facing website process.	Innovation	10/19/2015	6/30/2017	273	12/31/2018

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
2	The COO should coordinate with the CIO, Office of Presidential Libraries and the CINO to develop and document a centralized process to manage the public facing websites.	Innovation	10/19/2015	6/30/2017	273	12/31/2018
3	The CIO and CINO should clearly define the roles and responsibilities throughout the process developed in recommendation #2.	Innovation	10/19/2015	6/30/2017	273	12/31/2018
5	The CIO and NGC should review and document the approval of all agreements for web hosting services.	Information Services	10/19/2015	6/30/2017	92	6/30/2019
6	The CIO should review all of the systems attached to the NARANet general support system to determine if there are any others that are not FISMA compliant.	Information Services	10/19/2015	6/30/2017	92	6/30/2019
7	The CIO should coordinate with the CINO to make the web hosting environment FISMA compliant.	Information Services	10/19/2015	6/30/2017	92	6/30/2019
8	The COO should coordinate with the CIO and CINO to evaluate whether all of the web hosting environments (internal and external) should be consolidated into one centralized system for FISMA purposes.	COO	10/19/2015	6/30/2017	273	12/31/2018
10	The CIO should provide Innovation with guidance that clearly delineates the management responsibilities of the web hosting environment between Information Services and Innovation.	Information Services	10/19/2015	6/30/2017	92	6/30/2019
12	The CIO, COO, and CINO should retroactively perform or obtain from the contractor, vendor, or partner IT security assessments on vendors that currently host NARA websites.	Information Services	10/19/2015	6/30/2017	92	6/30/2019

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
13	The CIO should require an IT security assessment be performed prior to NARA initiating a web hosting agreement.	Information Services	10/19/2015	6/30/2017	92	6/30/2019
14	The CIO should ensure that all IT service agreements with external contractors, vendors, or partners have a clause that requires NARA or an independent third-party contractor to annually perform IT security assessments on contractor's, vendor's and partner's external web hosting environment(s) that host NARA websites.	Information Services	10/19/2015	6/30/2017	92	6/30/2019
15	The CIO should ensure Information Services personnel document their review of the IT security assessments.	Information Services	10/19/2015	6/30/2017	92	6/30/2019
16	The CIO should ensure Information Services include an audit clause in the agreement that requires contractors, vendors, and partners to provide all documentation to the OIG without requiring a signed NDA.	Information Services	10/19/2015	8/31/2017	92	6/30/2019
17	Develop a process for managing access to shared user accounts.	Information Services	10/19/2015	8/31/2017	92	6/30/2019
18	Implement the annual compliance check required by the User Account Management Standard Operating Procedure for Administrator accounts to the shared user accounts.	Information Services	10/19/2015	6/30/2017	92	6/30/2019
24	Apply the baseline configuration to the web servers.	Information Services	10/19/2015	6/30/2017	92	6/30/2019
26	The CIO should require all systems develop a baseline configuration document and have it approved before it is applied to the entire system.	Information Services	10/19/2015	6/30/2017	92	6/30/2019

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
28	This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.	Information Services	10/19/2015	6/30/2017	92	6/30/2019
29	This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.	Information Services	10/19/2015	6/30/2017	92	6/30/2019
30	This recommendation contains information about IT deficiencies which, if made public, could endanger NARA systems. Please contact the OIG if you need further information.	Information Services	10/19/2015	6/30/2017	92	6/30/2019
	Oversight of FY2015 FISMA Assessment (16-02)					
1	For systems utilized by NARA and managed by Cloud Service Providers, NARA should develop and implement formalized procedures to ensure controls for which NARA has a shared responsibility are reviewed on an annual basis, documented and assessed as to the impact to NARA of any risks that may be present.	Information Services	1/16/2016	3/31/2017	913	No Change
2	NARA should complete the development, approval and deployment of baseline configurations which are currently in progress and ensure that systems are configured in accordance with best practices (including NIST-approved baselines), to include, but not limited to, always changing default credentials at the time of implementation.	Information Services	1/16/2016	3/31/2017	913	No Change

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
4	NARA should develop, update and implement formalized access control policies and procedures for the B&A, RRS, SCTS and DCU systems.	Information Services	1/16/2016	5/31/2017	852	No Change
8	NARA should develop, update and implement formalized VPN access policies and procedures to ensure individuals are granted appropriated access.	Information Services	1/16/2016	3/31/2017	913	No Change
13	For future agreements, NARA should: · require that providers of external information system services comply with NARA information security requirements. · define and document government oversight and user roles and responsibilities with regard to external information systems, and · establish a process to monitor security control compliance by external service providers on an ongoing basis.	Information Services	1/16/2016	5/31/2017	852	No Change
14	NARA should add an addendum to current agreements which requires compliance with NARA's information security requirements.	Information Services	1/16/2016	6/30/2017	822	No Change
20	NARA should implement the following corrective actions: · complete efforts to implement the Net IQ Sentinel product · develop and implement processes and procedures to monitor and at least weekly review user activity and audit logs (in accordance with NARA IT Security	Information Services	1/16/2016	3/31/2017	913	No Change

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
	Requirements), on the network, RRS, B&A, ENOS-HMS and DCU systems that may indicate potential security violations · Ensure the procurement of new IT system hardware and software, which provides user authentication, includes a minimum set of audit logging controls and functionality in accordance with NARA's IT Security Requirements, AU-2.					
	Audit of NARA's Public Facing Websites (16-05)					
1a	The CINO should coordinate with the CIO to improve NARA's management and internal controls surrounding the security of NARA's publicly-accessible websites. Specifically, we recommend the CINO coordinate with the CIO on the development of policies and procedures for secure website design and implementation that apply to all NARA publicly-accessible websites.	Innovation	3/25/2016	3/31/2017	273	12/31/2018
1b	The CINO should coordinate with the CIO to improve NARA's management and internal controls surrounding the security of NARA's publicly-accessible websites. Specifically, we recommend the CINO coordinate with the CIO to ensure all publicly-accessible websites are compliant with NIST SP 800-53 revision 4.	Innovation	3/25/2016	3/31/2017	-458	12/31/2020
1c	The CINO should coordinate with the CIO to improve NARA's management and internal controls surrounding the security of NARA's publicly-accessible websites. Specifically, we recommend the CIO regularly (at least quarterly) conducts a comprehensive web vulnerability scan on all NARA publicly-accessible websites.	Information Services	3/25/2016	12/31/2016	92	6/30/2019

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
1d	The CINO should coordinate with the CIO to improve NARA's management and internal controls surrounding the security of NARA's publicly-accessible websites. Specifically, we recommend the CIO documents the process conducting a web vulnerability scan on all publicly-accessible websites.	Information Services	3/25/2016	12/30/2016	92	6/30/2019
1e	The CINO should coordinate with the CIO to improve NARA's management and internal controls surrounding the security of NARA's publicly-accessible websites. Specifically, we recommend the CIO provides the necessary training to IT Security personnel to be able to review and interpret the vulnerability scanner results.	Information Services	3/25/2016	3/31/2017	92	6/30/2019
1g	The CINO should coordinate with the CIO to improve NARA's management and internal controls surrounding the security of NARA's publicly-accessible websites. Specifically, we recommend the CIO requires all NARA publicly-accessible websites to apply NARA's password configuration requirements.	Information Services	3/25/2016	3/31/2017	92	6/30/2019
1i	The CINO should coordinate with the CIO to improve NARA's management and internal controls surrounding the security of NARA's publicly-accessible websites. Specifically, we recommend the CIO requires users to change their passwords after a website password reset.	Information Services	3/25/2016	3/31/2017	92	6/30/2019
1j	The CINO should coordinate with the CIO to improve NARA's management and internal controls surrounding the security of NARA's publicly-accessible websites. Specifically, we recommend the CIO analyzes all publicly-accessible websites to determine if they are	Information Services	3/25/2016	2/28/2017	92	6/30/2019

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
	vulnerable to all variations of cross-site scripting including reflected.					
1k	The CINO should coordinate with the CIO to improve NARA's management and internal controls surrounding the security of NARA's publicly-accessible websites. Specifically, we recommend the CINO coordinates with the CIO to review all publicly-accessible websites for any potential information that could affect NARA's IT security posture.	Information Services	3/25/2016	3/31/2017	92	6/30/2019
5	The CIO should document a process to review all security assessments by a qualified official.	Information Services	3/25/2016	2/28/2017	92	7/31/2019
6	The CIO should ensure Information Services personnel review all cloud hosting security assessments.	Information Services	3/25/2016	2/28/2017	92	7/31/2019
7	The CIO should ensure Information Services personnel document their review of the IT security assessments.	Information Services	3/25/2016	2/28/2017	92	7/31/2019
	Audit of Inadequate Information and Physical Security Controls at Select Federal Records Centers and Audit of NARA's Refile Processes at Selected Federal Records Centers (16-07)					
9	The Executive for Agency Services should implement standard IRS document locators at the FRCs.	Agency Services	5/17/2016	12/31/2017	183	3/31/2019
10	The Executive for Agency Services establish standardized policies and procedures for the quality control reviews at the FRCs, including: The selection criteria and quality control sample percentage to ensure the quality and timeliness of the quality control review. Physically checking some percentage of refiles selected for review to ensure they were properly refiled. Establishing timeframes for when the reviews must be	Agency Services	5/17/2016	9/30/2017	183	3/31/2019

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
	conducted. Documenting reviews performed, including records selected, errors identified, preparer and reviewer sign-off, and notification to employees and supervisors. Determining the appropriate method for reviewing interfiles. Ensuring different employees are responsible for the batching, selecting the quality control sample, refiling, and quality control review of records. A mechanism for tracking errors identified by employee and conducting periodic training when consistent errors are identified.					
11	The Executive for Agency Services should conduct training for all employees on the policies and procedures for quality control reviews, including notification of errors and penalties.	Agency Services	5/17/2016	12/31/2017	92	6/30/2019
12	The Executive for Agency Services should establish standardized policies and procedures for tracking and documenting IRS record problems, including problems with refiles. Identify timeframes for resolution and when the IRS should assist with resolution.	Agency Services	5/17/2016	6/30/2017	273	12/31/2018
13	The Executive for Agency Services should implement a mechanism (database, etc.) to facilitate the problem tracking and resolution process.	Agency Services	5/17/2016	6/30/2017	273	12/31/2018
Oversight of Enterprise-Wide Risk Assessment (17-AUD-01)						
1a	The Chief Operating Officer/Chief Risk Officer should fully implement all components of NARA 160, including developing, documenting, and fully implementing NARA 162, *NARA's Enterprise Risk Management*	CFO	10/28/2016	9/29/2017	92	6/30/2019

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
	Program. Within NARA 162, roles and responsibilities for ERM activities should be clearly identified.					
1b	The Chief Operating Officer/Chief Risk Officer should fully implement all components of NARA 160, including developing, documenting, and fully implementing NARA 163, *NARA's Issues Management*.	CFO	10/28/2016	9/29/2017	92	6/30/2019
2a	The Chief Operating Officer/Chief Risk Officer should develop, document, and implement a formal process to identify and prioritize risks within the organization. Risks should be tied directly to NARA's strategic plan and mission and prioritized based on their overall importance to the agency.	CFO	10/28/2016	9/29/2017	92	6/30/2019
2b	The Chief Operating Officer/Chief Risk Officer should develop, document, and implement a formal process to prioritize risk management activities, including the use of limited resources based on key risks within the organization. Management's prioritization should be clearly documented and include formal steps to ensure risks are maintained at an appropriate level.	CFO	10/28/2016	9/29/2017	92	6/30/2019
3	The Chief Operating Officer/Chief Risk Officer should provide additional resources to the Office of Accountability to ensure ICP activities are effectively carried out.	CFO	10/28/2016	9/29/2017	92	6/30/2019
4	The Chief Operating Officer\Chief Risk Officer develop and implement a formal process to review and evaluate the completeness and accuracy of ICP documentation submitted. Validation procedures should include a formal review: To ensure all required documentation has been	CFO	10/28/2016	9/29/2017	92	6/30/2019

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
	submitted by the due date. Where documentation has not been provided, NARA should have a formal process in place to follow up and obtain the required documentation. Of ICP documentation submitted to ensure it is both complete and accurate. Where discrepancies are identified, NARA should have a formal process in place to follow up with management so corrections can be made. Of each office's submission to determine whether risks identified and conclusions made are appropriately supported. Of test plans and test results for all high-risk or highly critical functions to ensure they clearly demonstrate the office's methodology for performing testing and reaching conclusions. Of monitoring plans and monitoring results for all functions that clearly show the extent of monitoring performed, the office's methodology for performing the monitoring, and the rationale for its conclusions.					
5	The Chief Operating Officer/Chief Risk Officer should develop and fully implement a formal ICP training program. NARA's ICP training program should identify and require individuals who are involved with NARA's ICP to complete initial training and refresher training periodically thereafter. Further, management should track completion of ICP training to ensure all individuals involved in the ICP process have received adequate training.	CFO	10/28/2016	9/29/2017	92	6/30/2019
	Audit of NARA's System Inventory (17-AUD-02)					

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
1	The CIO should develop, document, approve and implement a process for developing and maintaining the system inventory, in adherence to 44 U.S.C. § 3505(c).	Information Services	11/4/2016	5/1/2017	242	1/31/2019
2	The CIO should ensure all of the systems managed by NARA and its contractors are included in the inventory.	Information Services	11/4/2016	8/30/2017	214	2/28/2019
3	The CIO should update the inventory annually to ensure the information populated in the inventory is complete and accurate.	Information Services	11/4/2016	5/1/2017	214	2/28/2019
4	The CIO should document in NARA Directive 101 the organization responsible for maintaining the system inventory.	Information Services	11/4/2016	8/31/2017	214	2/28/2019
5	The CIO should comply with FIPS 199 and NIST SP 800-60 to ensure all information systems are categorized.	Information Services	11/4/2016	9/30/2017	273	12/31/2018
6	The CIO should comply with FIPS 199 and NIST SP 800-60 to ensure the categorization of information systems is accurate.	Information Services	11/4/2016	9/30/2017	273	12/31/2018
7	The CIO should update the FIPS 199 guidance to include all information types listed in NIST SP 800-60 Volume II.	Information Services	11/4/2016	9/30/2017	273	12/31/2018
8	The CIO should coordinate with system owners on validating their current FIPS 199 to ensure the systems categorization level is accurate.	Information Services	11/4/2016	12/30/2016	273	12/31/2018
Audit of NARA's Compliance with the Federal Managers Financial Integrity Act for FY15 (17-AUD-03)						
2	The Archivist should implement or upgrade current internal control software or utilize other mechanisms to	CFO	11/4/2016	9/29/2017	92	6/30/2019

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
	enhance and improve the agency's ability to track and report on internal controls.					
4	The Archivist should ensure the MCOC tracks and manages all high-level risks.	CFO	11/4/2016	9/29/2017	92	6/30/2019
5b	The Archivist should address outstanding recommendations from OIG Audit Report No. 13-01, including revisiting his decision on the placement and role in the organization of the Chief Risk Officer.	CFO	11/4/2016	9/29/2017	92	6/30/2019
6a	NARA Executives should ensure monitoring and testing plans are sufficiently reported in the ICP Tool.	CFO	11/4/2016	9/29/2017	92	6/30/2019
6b	NARA Executives should ensure results of monitoring and testing plans are achievable within the reporting timeframe. *Unresolved - The agency did not agree to implement the recommendation.*	CFO	11/4/2016	Unresolved	N/A	N/A
6c	NARA Executives ensure all information is up-to-date and reflects the current control environment.	CFO	11/4/2016	9/29/2017	92	6/30/2019
7	NARA Executives should identify, develop, and include in ICP reports measurable indicators to evaluate functions.	CFO	11/4/2016	9/29/2017	92	6/30/2019
8	NARA Executives should update NARA Directive 101 to include internal control responsibilities for each office.	CFO	11/4/2016	Unresolved	N/A	N/A

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
	Unresolved - The agency did not agree to implement the recommendation.					
9	The ICP Official develop and implement a consistent risk assessment process and format for risk ranking, analysis of effect or impact, and risk reporting.	CFO	11/4/2016	9/29/2017	92	6/30/2019
10	The ICP Official should review the ICP reports and make and document any revisions necessary to the format to ensure all necessary information is obtained in the reports.	CFO	11/4/2016	10/31/2017	92	6/30/2019
Audit of NARA's Management Control over Access Applications (17-AUD-04)						
2	The CIO should, in conjunction with each program office, implement the security assessment process as described in NARA's Enterprise Architecture to those applications/databases determined critical to carrying out NARA's or program offices' missions from Recommendation 1.	Information Services	11/18/2016	12/31/2017	273	12/31/2018
3	The CIO should, in conjunction with each program office, develop and implement a comprehensive, systematic process to determine when a MS Access application or database should be recognized as an IT system.	Information Services	11/18/2016	6/30/2017	273	12/31/2018
4	The CIO should, in conjunction with each program office, determine all MS Access databases containing PII and ensure they are: (a) encrypted in storage and transmission; and (b) password-protected in accordance with NARA Directive 1608 and the Privacy Act.	Information Services	11/18/2016	12/31/2017	304	11/30/2018

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
5	The CIO should, in conjunction with each program office, develop and implement a process, for future MS Access applications and databases created by program offices, including notification to and approval from the Office of Information Services for those that are mission-critical and/or contain PII or otherwise sensitive information.	Information Services	11/18/2016	4/30/2017	273	12/31/2018
	Audit of NARA's Procurement Program (17-AUD-06)					
3	The Chief Acquisition Officer (CAO) should formally appoint a Senior Procurement Executive (SPE) and procurement officials who are authorized to approve warrants over $100,000,000 and approve warrant for construction and architectural-engineering services contracting officers.	CAO	11/15/2016	5/14/2017	273	12/31/2018
5	Competition Advocate, in collaborations with the CAO, should develop and implement procedures to promote the acquisition of commercial items and report annually new initiatives to the CAO and SPE.	CAO	11/15/2016	5/14/2017	273	12/31/2018
6	The CAO should develop and implement procedures to ensure contracting offices in Acquisitions Branch (BCN) and Space Planning and Projects Branch (BFS) report all contract related activity to the SPE.	CAO	11/15/2016	5/14/2017	-92	12/31/2019
7	The CAO should ensure NARA 501 NARA Procurement policy and NARA's General Acquisition Policy addresses procurements related to Architecture/Engineering and Construction.	CAO	11/15/2016	5/14/2017	-92	12/31/2019
8	The CAO should, in collaboration with CFO, Director of Acquisitions, and program managers, develop and	CAO	11/15/2016	5/14/2017	273	12/31/2018

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
	implement procedures for proper planning of new contracts with NARA funds.					
9	The CAO should develop and implement procedures to ensure contracts are evaluated to identify contracts that are wasteful, inefficient, or unlikely to meet NARA needs.	CAO	11/15/2016	5/14/2017	-92	12/31/2019
10	The CAO and SPE should develop and implement test plans and procedures to assess internal control over acquisition activities and programs using OMB Memorandum, *Conducting Acquisition Assessments*.	CAO	11/15/2016	5/14/2017	-92	12/31/2019
11	The CAO should modify procedures to ensure all contracting activity, including Architecture/ Engineering, construction services are included in random selections for internal control reviews.	CAO	11/15/2016	5/14/2017	273	12/31/2018
13	The CAO should include Contracting Officers who are not GS1102's, Contracting Officer Representatives and Program and Project Managers in the internal control program test plan.	CAO	11/15/2016	5/14/2017	-92	12/31/2019
14	The CAO should establish various performance metrics to be tracked and analyzed on how long the acquisition takes, where delays occur and why delays occur.	CAO	11/15/2016	5/14/2017	273	12/31/2018
15	The CAO should develop and implement meaningful and measurable performance metrics to continually assess the performance of the acquisition function in supporting NARA's mission and achieving acquisition goals.	CAO	11/15/2016	5/14/2017	273	12/31/2018

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
16	The CAO should ensure NARA 501 NARA Procurement policy include guidance to program offices on their responsibilities in the procurement process.	CAO	11/15/2016	5/14/2017	273	12/31/2018
18	The CAO should assess staffing needs for NARA's Procurement Program to ensure the procurement program has sufficient staff to maintain effective, efficient operations and adhere to Federal and internal guidance.	CAO	11/15/2016	5/14/2017	273	12/31/2018
19	The CAO should develop a process to monitor the close-out of contracts process to ensure contracts are closed in a timely manner and identify reasons contracts are not closed out in a timely manner.	CAO	11/15/2016	5/14/2017	-92	12/31/2019
20	The Acquisition Career Manager (ACM) should verify all contracting officers, contracting officer representatives, program and project managers, and other contracting professionals set up an account in Federal Acquisition Institute Training Application System for tracking certifications and continuous training.	CAO	11/15/2016	5/14/2017	-92	12/31/2019
23	The ACM should ensure NARA Certification for Program and Project Managers Applications are signed by the Deputy Archivist in accordance with NARA policy and maintained.	CAO	11/15/2016	5/14/2017	-92	12/31/2019
24	The CAO should ensure all contracting officers, regardless of their government series, be certified at an appropriate level; and any contracting professional issued an unlimited warrant be level III certified.	CAO	11/15/2016	5/14/2017	273	12/31/2018
25	The CAO should establish and implement procedures for potential administrative or disciplinary actions for contracting officers, and contracting officer	CAO	11/15/2016	5/14/2017	-92	12/31/2019

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
	representatives, and other contracting professionals that do not have their Federal Acquisition Certifications or continuous trainings required by OMB guidance. For example, if after one year from notice the contracting professional still does not have appropriate certificates and/or training, disciplinary action, removal of warrant or removal from the position may occur.					
26	The CAO should ensure there is more IT training for CO's that do a significant amount of work in IT in accordance with OMB technology acquisition cadre guidance.	CAO	11/15/2016	5/14/2017	-92	12/31/2019
Audit of NARA's Compliance with HSPD-12 (17-AUD-07)						
2	Chief of Management and Administration or designee should develop a detailed implementation plan with remaining work to be completed, critical tasks, roles and responsibilities of key personnel, milestones for critical tasks, costs, locations, and any other necessary documentation that would allow the agency to successfully implement Homeland Security Presidential Directive 12 (HSPD-12).	Information Services	2/19/2017	12/29/2017	640	No Change
3	Chief of Management and Administration or designee should use existing budgetary resources to fully implement HSPD-12.	Information Services	2/19/2017	12/29/2017	640	No Change
4	Chief of Chief of Management and Administration or designee should establish a reasonable date to fully implement HSPD-12.	Information Services	2/19/2017	12/29/2017	640	No Change
Audit of NARA's Adoption and Management of Cloud Computing Activities (17-AUD-08)						

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
1	The CIO should, acting as the centralized authority for NARA's cloud computing program, should take the lead and collaborate with business areas such as Acquisitions and General Counsel, to develop, approve, and implement comprehensive policies and procedures which will coordinate activities and establish key control points for NARA's cloud computing program.	Information Services	3/15/2017	12/29/2017	183	3/31/2019
2	The CIO should complete and document a review of existing IT systems for cloud compatibility.	Information Services	3/15/2017	12/29/2017	183	3/31/2019
3	The CIO should update the Enterprise Cloud Strategy with clearly defined roles and responsibilities, and develop and implement a written plan to execute the strategy.	Information Services	3/15/2017	12/29/2017	183	3/31/2019
4	The CIO should conduct and document a risk assessment specific to NARA's implementation of cloud computing in coordination with NARA's Chief Risk Officer.	Information Services	3/15/2017	12/29/2017	183	3/31/2019
5	The CIO should develop, approve, and implement written NARA-wide standards for the early identification and designation of cloud computing services, and consistently communicate the standard to those who need it.	Information Services	3/15/2017	12/29/2017	183	3/31/2019
6	The CIO should establish and approve a centralized reporting point for cloud computing inventory and develop, implement and communicate a written mechanism to standardize tracking cloud computing inventory across NARA's business area lines.	Information Services	3/15/2017	12/29/2017	183	3/31/2019
7	The CIO should coordinate with necessary business areas including Acquisitions and General Counsel to develop,	Information Services	3/15/2017	12/29/2017	183	3/31/2019

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
	approve, and implement its written cloud provisioning guidelines.					
8	The CIO should coordinate with necessary business areas including Acquisitions and General Counsel to develop, approve, and implement its IT Security Contractual Requirements in addition to a method to monitor and enforce the use of the standards.	Information Services	3/15/2017	12/29/2017	183	3/31/2019
9	The CIO, in conjunction with Acquisitions and General Counsel should develop, approve, and implement written standards for centralized maintenance and standardized monitoring of service level agreements and formally communicate the requirement to those who need it.	Information Services	3/15/2017	12/29/2017	183	3/31/2019
10	The CIO should coordinate with the Chief Acquisitions Officer, and General Counsel to establish a working group to evaluate and monitor recommendations and best practices for cloud computing procurement in order to improve the content and effectiveness of the CPIC Business Case Form.	Information Services	3/15/2017	6/30/2018	183	3/31/2019
Audit of NARA's Online Access to Digitized Holdings (17-AUD-12)						
5	The Chief Innovation Officer and Chief Information Officer develop a strategy to optimize the use of NARA's Cloud infrastructure as it pertains to providing online access to NARA's digitized holdings.	Innovation	6/19/2017	12/31/2018	183	3/31/2019
Audit of NARA's FOIA Program (17-AUD-16)						

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
9	Utilize updated processing mechanisms or processes to increase the efficiency and effectiveness of the FOIA Program.	NGC	9/27/2017	12/31/2019	-92	No Change
10	Develop an agency wide FOIA technology system or process that would enable coordination between components, provide document management and sharing, and standardized tracking and reporting of FOIA request.	NGC	9/27/2017	12/31/2018	273	No Change
DATA Act Audit (18-AUD-02)						
1	Monitor and evaluate steps already taken to reduce timing errors between FPDS and Prism.	CFO	11/8/2017	11/30/2017	669	No Change
2	Review and enhance the process to validate and reconcile data of contract and grant awardees, including demographic data, for all DATA Act files back to the source system on a regular basis and prior to file submission to USA Spending.	CFO	11/8/2017	3/31/2018	548	No Change
Audit of the Office of the Federal Register's Administration of the Electoral College Process (18-AUD-04)						
4	Obtain an independent authoritative review of the requirements in 3 U.S.C. § 6 and 11. Based on the outcome of the review, document the OFR's procedures for receiving certificates via registered mail.	Federal Register	2/26/2018	11/30/2018	304	No Change
5	Review ICP reports to ensure accuracy and documentation is available to support information documented in the quarterly reports.	Federal Register	2/26/2018	11/30/2018	-487	1/29/2021
Audit of NARA's Legacy Systems (18-AUD-06)						

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
1	The CIO develop a definition of a legacy system.	Information Services	3/29/2018	9/30/2019	0	No Change
2	The CIO in coordination with the program offices document when the system was put into production and the life expectancy of each system.	Information Services	3/29/2018	9/30/2018	365	No Change
3	The CIO in coordination with the program offices document the total cost to operate and maintain each system on an annual basis.	Information Services	3/29/2018	12/31/2018	273	No Change
4	The CIO create a centralized process to track legacy systems.	Information Services	3/29/2018	9/30/2018	365	No Change
5a	The CIO has visibility and access to all of NARA's systems. Specifically, we recommend the CIO coordinate with program offices to ensure visibility into all NARA systems.	Information Services	3/29/2018	9/30/2018	365	No Change
5b	The CIO has visibility and access to all of NARA's systems. Specifically, we recommend the CIO develop, document, and implement a policy to require program offices to annually report Information Systems to Information Services.	Information Services	3/29/2018	9/30/2018	365	No Change
5c	The CIO has visibility and access to all of NARA's systems. Specifically, we recommend the CIO document all NARA systems in the IT portfolio that is reported to OMB.	Information Services	3/29/2018	9/30/2019	0	No Change
5d	The CIO has visibility and access to all of NARA's systems. Specifically, we recommend the CIO ensure the total operation and maintenance costs of each system is documented, and reported to OMB.	Information Services	3/29/2018	9/30/2019	0	No Change

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
6	The CIO in coordination with System Owners Ensure all seven systems are adequately tracked, monitored, and the proper security controls are in place until they are subsumed within the ERA 2.0 project or other systems as planned.	Information Services	3/29/2018	9/30/2019	0	No Change
7	The CIO adhere to Title 40 U.S.C. §11312(b)(3) and require the cost and benefits of each alternative be documented and reviewed during the CPIC process.	Information Services	3/29/2018	9/30/2018	365	No Change
8	The CIO develop and implement an operational analysis policy as required by OMB 10-27.	Information Services	3/29/2018	9/30/2018	365	No Change
9	The CIO coordinate with each Program Office to conduct and document an operational analysis for IT investments currently in production in accordance with the policy in recommendation 8.	Information Services	3/29/2018	12/31/2019	-92	No Change
10	The CIO ensure risk assessments and risk assessment reports are completed and/or reviewed annually and updated accordingly for all NARA systems.	Information Services	3/29/2018	12/31/2019	-92	No Change
Audit of Human Capital Practices (18-AUD-09)						
1	The Chief of Management and Administration ensure all NARA Human Capital policies are reviewed, revised, finalized, and implemented.	CMA	6/4/2018	12/31/2020	-458	No Change
2	The Chief of Management and Administration ensure all electronic Official Personnel Folders for employees with previous federal employment have been transferred to NARA. Also, ensure all employee official records while employed at NARA are uploaded into the eOPF.	CMA	6/4/2018	12/31/2020	-458	No Change

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
3	The Chief of Management and Administration ensure a review of system data integrity is conducted and erroneous data is removed from Human Capital systems.	CMA	6/4/2018	12/31/2020	-458	No Change
4	The Chief of Management and Administration ensure all SCDs are accurate.	CMA	6/4/2018	12/31/2020	-458	No Change
	Audit of NARA's Processing of Textual Records (18-AUD-11)					
4	The Executive for Research Services: Revise Processing ICP Reports to comply with NARA Directive 161 internal control testing requirements.	Research Services	8/6/2018	6/28/2019	94	No Change
	Audit of NARA's Continuity of Operations (COOP) Readiness (18-AUD-14)					
2	The Chief Information Officer: determine the laptop computer needs for all current ERG, DERG, and RIT/RPT member employees, in consultation with Executives responsible for executing the PMEFs, MEFs, and ESAs for NARA; conduct a cost-benefit analysis for providing a government-furnished laptop computer to those employees identified from (a); and(c) provide a government-furnished laptop computer to the ERG, DERG, and RPT/RIT member employees, based on the analyses conducted from (a) and (b) above.	Information Services	8/20/2018	3/29/2019	185	No Change
7	The Chief Human Capital Officer, in coordination with Business Support Services, establish controls to ensure the accurate supervisor-employee relationship is reflected on the staff accountability tool.	Human Capital	8/20/2018	12/31/2018	273	No Change
15	The Chief Information Officer, in collaboration with Business Support Services as applicable, conduct a detailed review of the FIPS PUB 199 security	Information Services	8/20/2018	3/31/2020	-183	No Change

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
	categorization of all mission-critical systems identified from Recommendations 13 and 14 to ensure all of such systems are subject to appropriate contingency planning requirements documented in the NARA IT Security Methodology for Contingency Planning.					
16	The Chief Information Officer, in collaboration with Business Support Services as applicable, develop a procedure to review the reconciled list of mission-critical systems identified from Recommendations 13 and 14 above at least on an annual basis to re-evaluate the systems' mission-criticality, identify newly commissioned, mission-critical systems, and remove systems that have been decommissioned.	Information Services	8/20/2018	3/29/2019	185	No Change
19	The Chief Information Officer, in coordination with the Office of Federal Register, develop and implement a process to maintain an up-to-date security authorization package for the EFR system, which includes a system security plan, security assessment report, risk assessment report, plan of action and milestones (PO&M), contingency plan, contingency plan test, and business impact analysis.	Information Services	8/20/2018	3/31/2020	-183	No Change
20	The Chief Information Officer develop and implement a process to update the contingency plan, contingency plan test results, and business impact analysis on an annual basis for all information systems with a FIPS PUB 199 security categorization of moderate or high.	Information Services	8/20/2018	3/31/2020	-183	No Change
24	The Executive for Business Support Services, in coordination with Corporate Records Management, ensure NARA's essential COOP documents, including	Business Support Services	8/20/2018	9/30/2019	0	No Change

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
	COOP Plans, OEPs, PIPs, and REPs, are reviewed on an annual basis, updated as needed, and stored in designated electronic locations.					
25	The Executive for Business Support Services ensure Occupant Emergency Plans for all NARA sites, where NARA is a tenant agency, are provided to NARA's Designated Official for the site on an annual basis for review, update if necessary, and a signature.	Business Support Services	8/20/2018	9/30/2019	0	No Change
26	The Executive for Business Support Services, in coordination with Corporate Records Management, develop and implement a file structure to more effectively organize and manage current and non-current COOP documents for each MEF, ESA, and facility.	Business Support Services	8/20/2018	1/31/2019	242	No Change
27	The Executive for Business Support Services, in coordination with Corporate Records Management, Develop and implement a process to maintain version control and record of changes for revisions made to essential COOP documents and Emergency Response Plans.	Business Support Services	8/20/2018	9/30/2019	0	No Change
28	The Executive for Business Support Services, in coordination with Corporate Records Management, ensure all essential COOP documentation and their locations are reflected in CERIT.	Business Support Services	8/20/2018	4/30/2019	153	No Change
29	The Executive for Business Support Services review the training needs of staff in light of their comments in exercise AARs and either: (a) develop and implement the content and schedule of mission-specific COOP training to be provided to each NARA office on a periodic basis; or (b) develop and implement a systematic process to	Business Support Services	8/20/2018	3/29/2019	185	No Change

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
	ensure and all NARA employees take the correct, annual COOP training module commensurate with their roles and responsibilities, and accurately track the status based on the assigned roles.					
	Audit of NARA's FY 2018 Consolidated Financial Statements (19-AUD-01)					
1a	We recommend that the NARA Chief Information Officer continue to analyze and prioritize remediation efforts to accomplish security and control objectives. Key tasks should include, but are not limited to: Ensure user accounts are reviewed and disabled in accordance with NARA's information technology policies and requirements (repeat recommendation).	Information Services	11/8/2018	10/30/2020	-396	No Change
1c	We recommend that the NARA Chief Information Officer continue to analyze and prioritize remediation efforts to accomplish security and control objectives. Key tasks should include, but are not limited to: c. Ensure that all incidents are reported to US-CERT within one hour of discovery.	Information Services	11/8/2018	10/30/2019	-30	No Change
1d	We recommend that the NARA Chief Information Officer continue to analyze and prioritize remediation efforts to accomplish security and control objectives. Key tasks should include, but are not limited to: d. Ensure Security Assessment Reports are updated with summaries of test failures for all failed controls identified.	Information Services	11/8/2018	9/30/2019	0	No Change
1e	We recommend that the NARA Chief Information Officer continue to analyze and prioritize remediation efforts to accomplish security and control objectives. Key tasks should include, but are not limited to: e. Ensure security documentation such as system security plans are	Information Services	11/8/2018	10/30/2020	-396	No Change

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
	reviewed and updated on an annual basis, for each system (repeat recommendation).					
1f	We recommend that the NARA Chief Information Officer continue to analyze and prioritize remediation efforts to accomplish security and control objectives. Key tasks should include, but are not limited to: f. Ensure plans of actions and milestones are created, updated and remediated, for each system, in accordance with NARA policies, guidance and directives (repeat recommendation).	Information Services	11/8/2018	10/30/2020	-396	No Change
1g	We recommend that the NARA Chief Information Officer continue to analyze and prioritize remediation efforts to accomplish security and control objectives. Key tasks should include, but are not limited to: g. Implement remediation efforts to address security deficiencies identified during our assessments of NARA's database platforms and network infrastructure (repeat recommendation).	Information Services	11/8/2018	9/30/2019	0	No Change
1h	We recommend that the NARA Chief Information Officer continue to analyze and prioritize remediation efforts to accomplish security and control objectives. Key tasks should include, but are not limited to: h. Fully complete the migration of applications to vendor supported operating systems (repeat recommendation).	Information Services	11/8/2018	9/30/2019	0	No Change
1i	We recommend that the NARA Chief Information Officer continue to analyze and prioritize remediation efforts to accomplish security and control objectives. Key tasks should include, but are not limited to: i. Ensure all	Information Services	11/8/2018	9/30/2019	0	No Change

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
	changes are tested and properly approved before being moved into the production environment.					
	Audit of NARA's Compliance with FISMA (19-AUD-02)					
1	To assist NARA in strengthening its agency-wide information security program, CLA recommends the CIO ensure complete security authorization packages for each major application and general support system are completed prior to deployment into production.	Information Services	12/14/2018	10/30/2020	-396	No Change
2	To assist NARA in strengthening its agency-wide information security program, CLA recommends the CIO ensure SSPs are developed for all NARA systems in accordance with NARA policy.	Information Services	12/14/2018	10/30/2020	-396	No Change
3	To assist NARA in strengthening its agency-wide information security program, CLA recommends the CIO ensure SSPs are reviewed and updated for all NARA systems in accordance with NARA policy to ensure any missing control implementation details are completed, and missing privacy controls added.	Information Services	12/14/2018	10/30/2020	-396	No Change
4	To assist NARA in strengthening its agency-wide information security program, CLA recommends the CIO conduct risk assessments for each system in operation and establish policies or procedures to ensure that risk assessments are conducted at least annually.	Information Services	12/14/2018	10/30/2020	-396	No Change
5	To assist NARA in strengthening its agency-wide information security program, CLA recommends the CIO document summaries of test failures for all failed controls identified in Security Assessment Reports.	Information Services	12/14/2018	9/30/2019	0	No Change

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
6	To assist NARA in strengthening its agency-wide information security program, CLA recommends the CIO ensure all systems have POA&Ms created when weaknesses are identified, to include completion dates; are remediated timely; and are updated to include detailed information on the status of the corrective actions.	Information Services	12/14/2018	10/30/2020	-396	No Change
8	To assist NARA with strengthening its policy and procedure development and authorization controls, CLA recommends the Chief Information Officer in coordination with Strategy and Performance staff ensure IT policies, procedures, methodologies and supplements are reviewed and approved in accordance with NARA Directive 111.	Information Services	12/14/2018	9/30/2019	0	No Change
9	To assist NARA with strengthening its ISSO management controls, CLA recommends the CIO assign ISSO's for all major applications and general support systems.	Information Services	12/14/2018	9/30/2019	0	No Change
11	To assist NARA with strengthening its baseline configuration management controls, CLA recommends the CIO ensure reviews of baseline configurations are performed on an annual basis and updated as necessary.	Information Services	12/14/2018	9/30/2019	0	No Change
12	To assist NARA with strengthening its vulnerability management controls, CLA recommends the CIO Implement improved processes to remediate security deficiencies on NARA's network infrastructure, to include enhancing its patch and vulnerability management program to address security deficiencies	Information Services	12/14/2018	9/30/2019	0	No Change

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
	identified during our assessments of NARA's applications and network infrastructure.					
13	To assist NARA with strengthening its vulnerability management controls, CLA recommends the CIO Ensure all information systems are migrated away from unsupported operating systems to operating systems that are vendor-supported.	Information Services	12/14/2018	9/30/2019	0	No Change
14	To assist NARA in continuing to strengthen user authentication controls, CLA recommends the CIO ensures multi-factor authentication is enforced for all users with (a) network access via privileged accounts, (b) network access to data requiring moderate or high confidentiality; and/or (c) local access to non-privileged accounts or data, which require high confidentiality.	Information Services	12/14/2018	10/30/2020	-396	No Change
15	To assist NARA in continuing to strengthen the identification and authorization controls, CLA recommends the CIO ensure user system accounts for all systems are periodically reviewed and automatically disabled in accordance with NARA policy.	Information Services	12/14/2018	10/30/2020	-396	No Change
16	To assist NARA in continuing to strengthen the identification and authorization controls, CLA recommends the CIO ensure upon termination of employment, all system access is disabled in accordance with the applicable system security plan defined period, as described under control PS-4 "Personnel Termination."	Information Services	12/14/2018	9/30/2019	0	No Change
17	To assist NARA in continuing to strengthen the identification and authorization controls, CLA	Information Services	12/14/2018	9/30/2019	0	No Change

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
	recommends the CIO ensure user access request forms are retained for each user account on all systems.					
18	To assist NARA in continuing to strengthen the elevated privileged user training controls, CLA recommends the Chief Information Officer ensure individuals assigned elevated privileges have their user accounts disabled if they have not completed their security awareness training by their scheduled completion date.	Information Services	12/14/2018	9/30/2019	0	No Change
20	To assist NARA in strengthening its audit logging processes, CLA recommends the CIO ensure audit logging is enabled for each major information system.	Information Services	12/14/2018	10/30/2020	-396	No Change
21	To assist NARA in strengthening its audit logging processes, CLA recommends the CIO ensure periodic reviews of generated audit logs are performed for each major information system.	Information Services	12/14/2018	10/30/2020	-396	No Change
22	To assist NARA in strengthening its user authentication controls, CLA recommends the CIO ensure password configuration settings for all major information systems are in accordance with NARA IT Security Requirements.	Information Services	12/14/2018	10/30/2020	-396	No Change
23	To assist NARA in strengthening its user authentication controls, CLA recommends the CIO ensure the use of shared/group accounts is restricted to only those users with a valid business justification, by enhancing user account review procedures to incorporate reviews of shared/group account membership and reasonableness.	Information Services	12/14/2018	12/31/2019	-92	No Change
24	To assist NARA in strengthening its user authentication controls, CLA recommends the CIO ensure a process is developed, documented and implemented to change	Information Services	12/14/2018	10/30/2020	-396	No Change

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
	passwords whenever users within shared/group accounts change.					
25	To assist NARA in strengthening the audit review, analysis and reporting process, CLA recommends the CIO Ensure incidents are reported to US-CERT within one hour of being identified by the CSIRT of all computer security incidents involving a NARA Information system, in accordance with NARA IT security requirements.	Information Services	12/14/2018	9/30/2019	0	No Change
26	To assist NARA in strengthening its contingency planning controls, CLA recommends the CIO develop, update and finalize information system contingency plans for all NARA systems.	Information Services	12/14/2018	10/30/2020	-396	No Change
27	To assist NARA in strengthening its contingency planning controls, CLA recommends the CIO test the contingency plans for all NARA systems to include documentation of test plans, results and any needed updates to the contingency plan, and establish controls to ensure annual testing of contingency plans.	Information Services	12/14/2018	10/30/2020	-396	No Change
	Audit of Presidential Libraries' Analog Processing (19-AUD-03)					
1	Implement procedures to ensure consistent implementation of NARA's Processing Policy across all Presidential Libraries.	LPM	12/20/2018	12/31/2019	-92	No Change
2	Implement procedures to ensure consistent and accurate reporting of basic processing totals across all Presidential Libraries.	LPM	12/20/2018	12/31/2019	-92	No Change

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
3	Direct all Presidential Libraries to assess their holdings to determine the correct percentage of basic processing work as stipulated in NARA's Analog Records Processing Policy.	LPM	12/20/2018	12/31/2019	-92	No Change
4	Implement procedures for quality control review of processed holdings across all Presidential Libraries.	LPM	12/20/2018	12/31/2019	-92	No Change
5	Implement procedures to require adequate support for ICP reporting.	LPM	12/20/2018	12/31/2019	-92	No Change
6	Identify digitization as a function of LP and follow all reporting instructions under NARA Directive 161 and related appendices.	LPM	12/20/2018	6/30/2019	-92	No Change
	Audit of NARA's Purchase Card Program (19-AUD-07)					
1a	Enhancing instructions to approving officials to look for sales tax paid by a cardholder, recurring purchases, and split purchases.	CFO	3/29/2019	11/30/2019	-61	No Change
1b	Enhancing the monitoring of the approving officials timely verification of purchase card transactions.	CFO	3/29/2019	11/30/2019	-61	No Change
1c	Documenting the monitoring of purchase card transactions to ensure cardholders' recover sales tax paid and/or make a good-faith attempt to recover sales tax paid.	CFO	3/29/2019	11/30/2019	-61	No Change
1d	Documenting the monitoring of purchase card transactions to ensure split purchases are not occurring.	CFO	3/29/2019	11/30/2019	-61	No Change

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
1e	Monitoring purchase card transactions to ensure separation of duties from authorizing the purchases and making purchases.	CFO	3/29/2019	11/30/2019	-61	No Change
2	Ensure Accounting Policy and Operations and Acquisitions purchase card policies are updated to reflect current practices.	CFO	3/29/2019	11/30/2019	-61	No Change
3	Ensure Accounting Policy and Operations and Acquisitions update the controls and the methods used to monitor controls associated with the purchase card program.	CFO, CAO	3/29/2019	11/30/2019	-61	No Change
4	Enforce the current policy of rescinding cardholder and approving official privileges if they fail to complete refresher training.	CAO	3/29/2019	11/30/2019	-61	No Change
5	Improve the alternate control by informing cardholders and approving officials months prior to the refresher training due date.	CAO	3/29/2019	11/30/2019	-61	No Change
Audit of NARA's Oversight of Electronic Records Management in the Federal Government (19-AUD-10)						
1	Recommend the Management Control Oversight Council consider reporting the Electronic Records Management deficiencies identified in the audit report as a material weakness under Federal Managers' Financial Integrity Act.	Agency Services	6/11/2019	12/31/2019	-92	No Change
2	Create a complete authoritative list of all active Federal agencies, including but not limited to Departments, agencies, sub-agencies, and or components subject to the Federal Records Act. This list should be updated periodically.	Agency Services	6/11/2019	1/31/2020	-123	No Change

Rec. No.	Recommendation Text	Office	Date Issued	Original Implementation Date	Days Past Due[1]	Revised Implementation Date
3	Upon completion of Recommendation 2, include all active Federal agencies subject to the Federal Records Act in the annual Records Management Self-Assessment survey.	Agency Services	6/11/2019	1/31/2020	-123	No Change
4	Complete validation and data entry of the legacy permanent disposition authorities into ERA in a timely manner.	Agency Services	6/11/2019	7/31/2020	-305	No Change
5	Until recommendation 4 is completed, review ERA and implement a plan to update CASPER to more accurately reflect all known active permanent electronic schedules to identify records overdue for transfer to NARA.	Research Services	6/11/2019	12/31/2020	-458	No Change
6	Review whether existing technology for identifying gaps in electronic record accessions is sufficient and if not request funding or identify another option to reasonably ensure permanent electronic records are identified, scheduled, and ultimately obtained by NARA.	Agency Services	6/11/2019	12/31/2020	-458	No Change
7	Update internal controls to reflect a measured and reasonable approach to reaching out to agencies with known overdue records.	Agency Services	6/11/2019	9/30/2019	0	No Change
8	Codify in CFR how often Federal agencies are required to review record schedules.	Agency Services	6/11/2019	12/31/2020	-458	No Change
9	Contact Federal agencies currently using record schedules approved before January 1, 1990 and require the schedules be reviewed.	Agency Services	6/11/2019	9/30/2020	-366	No Change
10	Develop a strategy to ensure annual inspections results are used to effectively mitigate threats and risk to federal agency electronic records activities.	Agency Services	6/11/2019	5/29/2020	-242	No Change

OIG Hotline

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

Electronically: OIG Referral Form

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