



OFFICE of INSPECTOR GENERAL  
NATIONAL ARCHIVES and RECORDS ADMINISTRATION  
8601 ADELPHI ROAD, COLLEGE PARK, MD 20740-6001  
[www.archives.gov/oig](http://www.archives.gov/oig)

March 15, 2017

**TO:** David S. Ferriero  
Archivist of the United States

**FROM:** James Springs *James Springs*  
Inspector General

**SUBJECT:** *Audit of NARA's Adoption and Management of Cloud Computing*

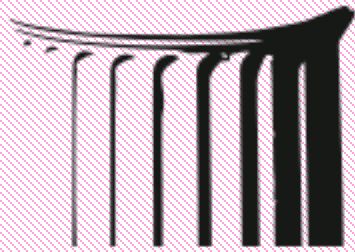
This memorandum transmits the results of our final report, for the *Audit of NARA's Adoption and Management of Cloud Computing* (OIG Audit Report No. 17-AUD-08). We have incorporated the formal comments provided by your office.

The report contains ten recommendations aimed at improving NARA's cloud computing activities. Your office concurred with all recommendations. Based on your March 9, 2017 response to the final draft report, we consider all the recommendations resolved and open. Once your office has fully implemented the recommendations, please submit evidence of completion of agreed upon corrective actions so that recommendations may then be closed.

As with all OIG products, we determine what information is publicly posted on our website from the attached report. Accountability has stated NARA does not desire any redactions to the posted report.

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

We appreciate the cooperation and assistance NARA extended to us during the audit. Please call me with any questions, or your staff may contact Jewel Butler, Assistant Inspector General of Audits, at (301) 837-3000.



OFFICE *of*  
INSPECTOR GENERAL  
NATIONAL ARCHIVES

Audit of NARA's Adoption and Management of  
Cloud Computing

March 15, 2017

OIG Audit Report No. 17-AUD-08

## Table of Contents

---

<b>Executive Summary</b> .....	3
<b>Background</b> .....	4
<b>Objectives, Scope, Methodology</b> .....	7
<b>Audit Results</b> .....	9
Finding 1. NARA’s cloud computing approach lacked maturity and adequate planning.....	9
Recommendations.....	15
Finding 2. NARA lacked an accurate cloud computing inventory.....	18
Recommendations.....	22
Finding 3. NARA executed cloud contracts without established standards in place.....	23
Recommendations.....	28
Finding 4. CPIC’s Business Case Form could be improved. ....	30
Recommendations.....	31
<b>Appendix A – NARA Identified Cloud Computing Risks</b> .....	33
<b>Appendix B – Examples of Internal Definitions and Designations of Cloud Computing at NARA</b> .....	35
<b>Appendix C – Examples of External Terminology, Definitions and Designations of Cloud Computing</b> .....	36
<b>Appendix D – Potential Future Audit Work</b> .....	38
<b>Appendix E – Acronyms</b> .....	39
<b>Appendix F – Management Response</b> .....	40
<b>Appendix G – Report Distribution List</b> .....	44

# Executive Summary

## *Audit of NARA's Adoption and Management of Cloud Computing*

OIG Audit Report No. 17-AUD-08

March 15, 2017

### **Why Did We Conduct This Audit?**

The OMB directed agencies to shift to a “Cloud First” policy over six years ago on December 9, 2010. NARA reported moving services to the cloud as early as 2011, and like other federal agencies continues to evaluate existing and new services for cloud computing opportunities, increasing spending on cloud computing annually.

The opportunities presented in the paradigm of cloud computing also present unique challenges to agencies in meeting federal government requirements – a contract can quickly become an impediment to successful implementation of cloud computing. Recent news headlines demonstrate the pitfalls. For example, a federal appeals court ruled American companies do not have to hand over customer data to U.S. police if it's stored on computers in another country. We performed this audit to evaluate NARA's cloud computing environment and determine whether NARA was properly prepared to manage its transition to cloud computing services and meet OMB's goals of a “Cloud First” policy.

### **What Did We Recommend?**

NARA needs to develop and implement a standard and comprehensive approach to its cloud computing activities, coordinating processes across business lines. This report makes 10 recommendations, which are intended to improve the performance of NARA's cloud computing program.

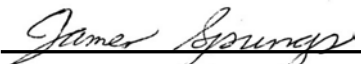
### **What Did We Find?**

NARA's approach to cloud computing lacked maturity and adequate planning. We found NARA moved multiple systems to the cloud without properly considering whether or not the applicable organizations were pragmatically ready to migrate services to the cloud. This occurred because NARA lacked a centralized authority point with adequate resources to conduct the planning and provide the direction necessary for NARA's transition to cloud computing. As a result, NARA was not appropriately positioned to fully realize the benefits of cloud computing and meet OMB's “Cloud First” policy.

NARA lacked an accurate cloud computing inventory. NARA maintained several differing inventory listings and had not established an effective method to accurately inventory its cloud computing services. This occurred because NARA lacked a common identifier and designation for its cloud computing services, and the use of a centralized reporting point for those services. As a result, it will be difficult for NARA to apply the controls needed for the unique environment of cloud computing. This will also impair NARA's ability to accurately report performance information related to its cloud computing activities.

NARA executed cloud contracts without established standards in place. Despite years of implementing cloud computing contracts, NARA did not yet have an approved requirement to include a common set of procedures for CSPs to follow, including expected levels of service, as part of its cloud computing contracts. No reviews were conducted to determine the extent of contracts that may be without SLAs. In addition, NARA's approach to monitoring service levels lacked policies and procedures for a centralized monitoring method for its cloud contracts and lacked a central location for maintaining reports. Further, NARA was executing its cloud computing contracts without approved standards for contractual language. NARA did not consider development of cloud provisioning guidelines a priority, which may have impaired NARA's ability to establish effective controls and monitor service levels of cloud computing contracts. As a result, NARA may not be able to consistently and accurately measure the performance levels of NARA's cloud computing contracts in order to achieve the full benefits of a “Cloud First” policy.

Additionally, CPIC's Business Case Form could be improved. The design and content of CPIC's Business Case form did not allow for consistent and comprehensive collection of information needed for proposed IT investments. This occurred because CPIC did not incorporate relevant guidance and best practices for IT acquisitions into the content of the form. The form used lacked formal approval and was part of a temporary directive for interim guidance from FY 2012, NARA 801-3, *Temporary Capital Planning and Investment Control Process*, September 17, 2014. As a result, CPIC's Business Case Form was not as effective as it could be at capturing beneficial information on NARA's cloud computing activities. This may impair NARA's ability to make decisions which ensure IT projects align with NARA's mission and strategic goals. Further, NARA may not be fully considering the benefits of FedRAMP's “do once, use many times” approach.

  
James Springs  
Inspector General

## Background

---

In December 2010, the OMB announced its *25-Point Implementation Plan to Reform Federal Information Technology Management*, focusing on reforms to eliminate barriers and more effectively manage IT programs throughout the federal government. OMB's plan prompted NARA and other federal agencies to seek opportunities for cloud computing; a service-based alternative to in-house computing considered to be economical, flexible and fast. Agencies were to immediately shift toward a "Cloud First" policy, and begin by identifying and moving at least three cloud computing capable services within their organizations to the cloud by June 2012. At the time OMB issued its Cloud Computing Strategy in 2011, the federal government expected an estimated \$20 billion (25%) of its \$80 billion in IT spending was a potential target for migration to cloud computing solutions. According to OMB, in FY 2017 federal agencies plan to increase IT spending to an estimated \$89.9 billion, of which over \$7.5 billion is expected to be provisioned services, which includes cloud services.<sup>1</sup> In line with this trend, NARA expects to continue increasing its move to cloud services. Since OMB's direction, NARA has moved a considerable amount of services to the cloud, including those related to email, human resources, webhosting, capital planning, security clearance tracking, and IT help desk operations. Recently NARA announced an Enterprise Cloud Services contract to help its Information Services (I) division meet long-term goals, such as increasing capacity to host and store digital content in the cloud.

The recent passing of the *Modernizing Government Technology Act of 2016*, September 26, 2016 (MGT Act), will further accelerate agencies' move to the cloud. In addition to assisting the Federal Government in modernizing federal Information Technology (IT), and incentivizing cost savings in federal IT through modernization, the MGT Act is intended to accelerate the acquisition and deployment of modernized IT solutions, such as cloud computing, by addressing impediments in the areas of funding, development, and acquisition practices.

Limited guidance for cloud computing was available to federal agencies when OMB issued its 25-Point Implementation Plan in 2010. When the *Federal Cloud Computing Strategy* emerged in February 2011, it represented the first step in providing guidance to Federal agencies on successfully implementing the "Cloud First" policy. Additional guidance followed from the National Institute of Standards and Technology (NIST), the Chief Information Officer Council (CIOC), the Chief Acquisition Officers Council (CAOC), the Federal Risk and Authorization Management Program (FedRAMP), and OMB. These included the *NIST Definition of Cloud Computing*, *NIST Cloud Computing Standards Roadmap*, *CIOC/CAOC Best Practices for Acquiring IT as a Service*, and *FedRAMP Standard Contract Language*.

---

<sup>1</sup> <https://itdashboard.gov/drupal/summary/000>

NIST's definition of cloud computing states it is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Service models include Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). The models and variants available represent both opportunities and risks which impact an agency's ability to control the environment. Each service model offers unique functionality depending on the class of user, with control of the environment decreasing as one moves from Infrastructure to Platform to Software.

Prior audits, reviews, and news headlines have highlighted issues commonly associated to federal agencies' cloud computing activities. For example, contracts represent particular risks to federal agencies when they do not account for components such as data residing outside the boundaries of the United States. Most recently, a federal appeals court ruled in July 2016, that an American company did not need to hand over customer data to U.S. police in response to a warrant if it was stored on computer servers in Ireland.<sup>2</sup> The Council of Inspectors General on Integrity and Efficiency's (CIGIE) *Cloud Computing Initiative*, September 2014, evaluated 19 participating federal agencies' efforts when adopting cloud computing technologies. Among the findings, 9 of 19 agencies reported they did not have an accurate inventory of their cloud systems. All 77 contracts evaluated under the initiative lacked the detailed specifications recommended in Federal cloud computing guidelines and best practices documentation.<sup>3</sup> Though NARA's Office of Inspector General (OIG) did not participate in the CIGIE initiative, prior audit work identified that NARA did not require external vendors or partners to conduct and provide security assessments of the systems hosting NARA websites.<sup>4</sup> In addition, the FY 2015 Federal Information Security Modernization Act (FISMA)<sup>5</sup> audit revealed some agreements between NARA and vendors of contractor hosted systems (e.g. Google and SCTS) did not include a clause requiring these providers of external information system services to comply with NARA security requirements and employ appropriate security controls which are effectively implemented and compliant with FISMA requirements, OMB policy, and applicable NIST guidelines.

---

<sup>2</sup> <http://money.cnn.com/2016/07/14/technology/microsoft-ireland-privacy/>

<sup>3</sup> [https://www.ignet.gov/sites/default/files/files/Cloud%20Computing%20Initiative%20Report\(1\)\(1\).pdf](https://www.ignet.gov/sites/default/files/files/Cloud%20Computing%20Initiative%20Report(1)(1).pdf)

<sup>4</sup> <https://www.archives.gov/oig/pdf/2016/audit-report-16-01.pdf>

<sup>5</sup> In general, the head of each agency shall be responsible for providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—information collected or maintained by or on behalf of the agency; and information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of the agency.

A key component in implementing effective controls is the control environment. Governance plays a significant role in an agency's ability to provide the control and oversight necessary for effective programs and operations. According to NIST:

“governance implies control and oversight by the organization over policies, procedures, and standards for application development and information technology service acquisition, as well as the design, implementation, testing, use, and monitoring of deployed or engaged services. With the wide availability of cloud computing services, lack of organizational controls over employees engaging such services arbitrarily can be a source of problems. While cloud computing simplifies platform acquisition, it doesn't alleviate the need for governance; instead, it has the opposite effect, amplifying that need.”

At NARA, Information Services holds primary responsibility for administering the agency's cloud computing activities. The Chief Information Officer (CIO) provides executive oversight for Information Services. The Deputy CIO sees himself as the sponsor of NARA's cloud computing program and provides leadership for NARA's Enterprise Cloud Services Program, while a Program Manager from the Portfolio Management Division is also responsible for a portion of NARA's cloud computing program. Within Information Services, the Capital Planning and Investment Control (CPIC) Manager sets the policy and process, guides people through the CPIC process, coordinating with Acquisitions, and conducts reporting on cloud services at NARA. Within Business Support Services (BCN), a Contracting Officer (CO) for NARA's Acquisition Branch handles management of software contracts, while IT Operations handles monitoring of infrastructure and platform contracts. These duties are further delegated to CORs. At the time of fieldwork, NARA 101, Part 11.g.5, Business Support Services, October 18, 2015, stated Acquisition Management responsibilities included implementing procurement initiatives, best practices, and reforms, including developing a program for routine review and assessment of NARA contract and acquisition activities and determining specific areas where performance standards should be established and applied.<sup>6</sup> Attorneys from NARA's General Counsel assist with review of contracts and policy, and deal with legal issues which may arise. Additional staff from areas such as Investment Planning and Management, IT Security Management Division, IT Operations Division, Architecture and Technology Management Division, Development and Tools Management Division, and Portfolio Management Division also hold assigned responsibilities impacting NARA's cloud computing activities.

---

<sup>6</sup> In updated NARA 101, Part 14, Office of the Chief Acquisition Officer, October 2, 2016, Chief Acquisition Officer duties include implementation of procurement initiatives, best practices, and reforms, including developing a program for routine evaluation of contract performance to identify contracts that are wasteful, inefficient, or unlikely to meet NARA needs and integrates the results of the evaluations into future award decisions; regularly reviews NARA acquisition activities to determine specific areas where performance standards should be established and applied. .

## Objectives, Scope, Methodology

---

### *Objective*

Our audit objective was to evaluate NARA's cloud computing environment. Specifically, to determine whether NARA was properly prepared to manage its transition to cloud computing services and meet OMB's goals of a "Cloud First" policy.

### *Scope and Methodology*

Numerous other Offices of Inspector General performed assessments of their respective agency's cloud computing efforts and compliance with a "Cloud First" policy. Our audit work explored whether NARA experienced strengths and weaknesses similar to other federal agencies, and focused on the governance of NARA's cloud computing activities. Though we considered the potential risks associated to NARA's cloud computing contracts, we will review these contracts in future work.

We obtained and reviewed applicable, laws, regulations, and guidance, as well as NARA's strategy, policies, procedures and other documents associated to the agency's governance of cloud computing, including but not limited to:

- a. *OMB 25 Point Implementation Plan to Reform Federal Information Technology Management*, December 9, 2010
- b. *OMB Federal Cloud Computing Strategy*, February 8, 2011
- c. *OMB Memorandum for Chief Information Officers, Security Authorization of Information Systems in Cloud Computing Environments*, December 8, 2011
- d. *Federal Acquisition Regulation (FAR) Clause 52.204-21, Basic Safeguarding of Covered Contractor Information Systems*, June 2016
- e. *FedRAMP Standard Contract Language*
- f. *General Services Administration (GSA) Whitepaper Best Practices for Effective Cloud Computing Services Procurement within the Federal Government*, January 2016
- g. *NIST SP 500-291, NIST Cloud Computing Standards Roadmap, Version 2*, July 2013
- h. *NIST SP 800-45 The NIST Definition of Cloud Computing*, September 2011
- i. *NIST SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing*, December 2011
- j. *NIST SP 800-146 Cloud Computing Synopsis and Recommendations*, May 2012
- k. *CIOC/CAOC Creating Effective Cloud Computing Contracts for the Federal Government, Best Practices for Acquiring IT as a Service*, February 24, 2012
- l. *NARA's Enterprise Cloud Strategy*, July 22, 2014



- m. NARA 801-3 *Temporary Capital Planning and Investment Control Process*, September 17, 2014
- n. NARA Draft *Standard IT Security Contractual Requirements for Unclassified Information/Information Systems*, April 16, 2016
- o. GAO *Standards for Internal Control in the Federal Government*, September 2014

In order to accomplish our objectives, we interviewed NARA management and personnel, including employees in the Office of the Chief Operating Officer, Business Support Services, and Office of the Archivist of the United States. We assessed NARA's inventory of cloud computing services and reviewed how NARA is managing these services. We also assessed NARA's progress of migrating to cloud technologies and how NARA identifies opportunities for shared services and cloud computing.

Our audit took place at National Archives II in College Park, Maryland. This performance audit was conducted in accordance with generally accepted government auditing standards between April 2015 and August 2016.<sup>7</sup> The generally accepted government auditing standards require we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The audit was conducted by Sonya Zacker, Senior IT Auditor.

---

<sup>7</sup> Due to the departure of the lead auditor, we placed a hold on the fieldwork which began in April 2015. Upon staff replacement, we reinitiated fieldwork in May 2016 with a new entrance conference.

## Audit Results

---

### **Finding 1. NARA’s cloud computing approach lacked maturity and adequate planning.**

NARA moved multiple systems to the cloud without properly considering whether or not the applicable organizations were pragmatically ready to migrate services to the cloud.<sup>8</sup> This occurred because NARA lacked a centralized authority point with adequate resources to conduct the planning and provide the direction necessary for NARA’s transition to cloud computing. Activities often crossed over key business areas, such as Information Services and Acquisitions, but lacked coordination. Although Information Services officials claimed responsibility for NARA’s cloud computing program, their business area suffered from numerous positional vacancies and confusion among its staff members about roles and responsibilities. Though NARA 101 for Information Services assigned responsibilities, we found officials were not always aware of their responsibilities under NARA 101. Roles within NARA 101 were often vacant and filled with acting roles. Even the CIO and Deputy CIO served in acting positions for the Portfolio Management Division and the Architecture and Technology Management Division, respectively. As a result, NARA was not appropriately positioned to fully realize the benefits of cloud and meet OMB’s “Cloud First” policy.

According to OMB’s *Federal Cloud Computing Strategy*, February 8, 2011, agencies should consider whether or not the applicable organization is pragmatically ready to migrate their service to the cloud.

GAO’s *Standards for Internal Control in the Federal Government*, September 2014, also known as the Green Book, states as programs change and entities strive to improve operational processes and implement new technology, management should continually evaluate its internal control systems so that it’s effective and updated when necessary.

The CIOC/CAOC *Best Practices for Acquiring IT as a Service*, February 24, 2012, highlights the importance of business area collaboration when acquiring cloud computing services. Proactive planning with all necessary stakeholders (e.g. chief information officers, general counsels, privacy officers, records managers, e-discovery counsel, Freedom of Information Act (FOIA)

---

<sup>8</sup> Systems included but were not limited to the Security Clearance Tracking System (SCTS), Google Apps for Government, Description and Authority Services (DAS), Online Public Access (OPA), Museum Collections Management Database (MCMD), Clarity PPM On Demand, Electronic Editing and Publishing System (eDocs), and RemedyForce.

officers, and procurement staff), is essential when evaluating and procuring cloud computing services.

### *Cloud Readiness*

According to OMB's *Federal Cloud Computing Strategy*, February 8, 2011, government services which have capable and reliable managers, the ability to negotiate appropriate service level agreements (SLA), related technical experience, and supportive change management cultures should receive a relatively high priority. Government services which do not possess these characteristics but are otherwise strong cloud candidates should take steps to alleviate any identified concerns as a matter of priority.

NARA's resource limitations contributed to NARA's latency to develop policies and procedures needed for cloud computing, and to NARA's latency to develop the documents needed to establish the direction for cloud transition. For example, we found key governance documents to be in draft or needing update. NARA's *Enterprise Cloud Strategy* Version 1.1, July 22, 2014, the *NARA Enterprise Architecture FY 2015 Agency Enterprise Roadmap*, May 18, 2015, and the *NARA System Development Life Cycle Methodology*, November 27, 2013 were in need of updates. NARA's *Cloud Security Architecture Reference*, March 2016 (also known as the Security Enclave) was still in draft, and updates were contingent on funding.

The IT Capital Planning Manager acknowledged they were still getting a lot of things ironed out. For example, the Enterprise Cloud Strategy did not reflect NARA's current governance process. The strategy did not include the addition of the Business Need Review Board (BNRB), the Stage Gate Review Board (SGRB) or NARA's reorganization of the Architecture Review Board (ARB) into the Investment Review Board (IRB). In addition, the IRB and Information Systems Steering Committee (ISSC) were operating without up to date charters. Documents needed to establish direction for the transition to cloud were also latent or out of date. For example, NARA was latent in developing a plan to execute its Enterprise Cloud Strategy. NARA had also not conducted a risk assessment specific to cloud computing. Further, NARA had not performed a comprehensive assessment of its on-premises systems for cloud compatibility.

NARA began reporting moving systems to the cloud as early as 2011. Similar to other agencies, NARA was not prepared for its implementation of cloud computing.<sup>9</sup> A NARA official stated there were lessons learned from a network outage, which highlighted a significant negative aspect of the growing trend toward cloud computing: the availability and reliability of network enabled IT services. The NARA official reported the most important "lesson learned" from that significant event – some applications were not appropriate for hosting in the cloud.

---

<sup>9</sup> [https://www.ignet.gov/sites/default/files/files/Cloud%20Computing%20Initiative%20Report\(1\)\(1\).pdf](https://www.ignet.gov/sites/default/files/files/Cloud%20Computing%20Initiative%20Report(1)(1).pdf)

NARA continued to report progress moving services to the cloud, such as Human Resources and Archives.gov, to the cloud in December 2012 and email by December 2013. NARA's most recent Strategic Plan, FY 2014 – FY 2018, included cloud computing among its opportunities and challenges, and stated NARA would meet the challenge by creating a strategy so that records created and used "in the cloud" could also be archived, preserved, and made publicly available in the cloud. In line with its strategy, NARA recently reported moving significant infrastructure and platform services to the cloud with an Enterprise Cloud Contract valued at approximately \$55 million. Further, NARA reported for FY 2016 and FY 2017, \$16.0 and \$17.2 million in provisioned services, respectively. However, NARA's Strategic Plan did not reflect the greater challenge in developing a programmatic approach to this transition, and a transition which should have been based upon a comprehensive evaluation of existing systems for cloud compatibility.

Further, when we asked for policies and procedures related to NARA's cloud computing activities in May 2016, a NARA official responded they were not applicable at the time. NARA lacked applicable contractual standards and maturity for its acquisition planning. For example, NARA drafted *Standard IT Security Contractual Requirements Unclassified*, April 18, 2016, however NARA was still reviewing the standards, and the standards were not approved as of November 2016. As part of a temporary directive, IT Capital Planning recently developed and began using an informal process, which requires evaluation of alternative services. We discuss these standards and the Capital Planning process later in this report.

#### *NARA's Enterprise Cloud Computing Strategy*

Despite the number of services moved to the cloud, NARA did not prepare an Enterprise Cloud Strategy until May 8, 2014, three and a half years after OMB required agencies to immediately shift to a "Cloud First" policy through the *25-Point Implementation Plan to Reform Federal Information Technology Management*. NARA had not updated the strategy in almost two years. We received no evidence the strategy was ever formally approved. Further, NARA still had no documented plan to execute the strategy.

NARA officials recognized that effective governance would be critical to the strategy's success. The first objective of the strategy was to foster a "cloud-first" (i.e.; service-based) approach for business initiatives requiring IT support. However, we found that NARA experienced difficulty executing the strategy. NARA's strategy was outdated and did not reflect departures and reassignments of major personnel. At least 9 of 12 stakeholders (75%) were either reassigned or left the agency. Though work had been done, such as developing a temporary CPIC process and a form to require consideration of cloud alternatives, NARA was late or had not taken action on some tasks. For example, NARA's *Cloud Security Architecture Reference* was in draft, dated March 2016, and completion was contingent upon funding. NARA's System Development Life Cycle Methodology, dated November 2013, was considered woefully inadequate and an update

was planned. In addition, NARA had not yet performed a risk assessment specific to cloud computing. Responsible NARA officials reported they were stretched thin and often performing in multiple roles. Some of the key factors in the strategy were listed as unfunded in NARA's draft *FY 2015 Agency Enterprise Roadmap*, May 18, 2015. The Deputy CIO explained some of these tasks were overcome by events, such as the NARANet Cloud Readiness Assessment and the cloud storage proof of concept, since they were obviously moving their operational system to the cloud and already deploying storage in the cloud.

We also identified a training risk which will impact NARA's ability to execute its strategy. Responsibilities for the NARA official serving as I's Enterprise Training Coordinator were still being developed. Although training is to be provided to Program and Project Managers, it will be a challenge because there is not a centralized reporting mechanism. The Training Coordinator cautioned that training needs to be part of the solicitation, and one of the contract deliverables.

Finally, NARA had not developed a detailed plan to execute the strategy. A NARA staff member stated NARA's immaturity regarding cloud computing activities is not for a lack of strategic thinking; the issues are 100 percent a lack of resources, and problems with Acquisitions to get contracts out and jobs posted. The staff member acknowledged the large amount of vacancies in various Information Services positions, as well as confusion with roles and responsibilities. Although roles and responsibilities should have been developed a year ago, Information Services had only recently met to develop a roles and responsibilities chart, as discussed later in this report.

We reviewed roles and responsibilities outlined in its documented policy, NARA 101, Part 10, Information Services, February 7, 2016, and found multiple vacancies, and responsibilities were poorly laid out and executed. For example, the Development and Tools Management Division responsibilities, which included key tasks to ensure systems and applications receive Authorizations to Operate (ATO), and ensure updates to NARA's System Development Life Cycle (SDLC) (NARA 805), were still under development and as yet undefined. A staff member from a separate division was taking on the task to update NARA's SDLC. Division level responsibilities were absent from the Portfolio Management Division, which housed the Program Management Branch and the newly proclaimed manager of the cloud computing program, which also lacked documented role and responsibilities. NARA staff we spoke with acknowledged confusion and tension about roles and responsibilities, and were often shouldering multiple responsibilities due to the amount of vacancies and understaffing, including those responsible for information services, acquisitions, risk management, contracting oversight duties, and program management. This impaired NARA's ability to effectively plan its transition to cloud computing.

### *Discussion with CIO*

When we discussed our concerns about the cloud strategy with NARA's CIO, we received a high-level update to the strategy outlining completed and expected accomplishments, as well as expected completion dates. The CIO reported they had already accomplished incorporating cloud into their governance structure, and brought on a subject matter expert (SME) for NARA's cloud environment. Though the addition of a SME will improve NARA's ability to manage its cloud computing activities, NARA is long overdue in addressing its latency to prepare for the transition to cloud computing. NARA has been slow to both develop and maintain items necessary for cloud readiness, and the CIO did not expect completion of significant milestones including finalizing plans to implement the 2011 Federal Computing Strategy, evaluating on-premises systems, and finalizing operational procedures until the first half of FY 2017.

According to GAO's Green Book, management should identify, analyze, and respond to significant changes that could impact the internal control system. Changes to internal conditions include changes to the entity's programs or activities, oversight structure, organizational structure, personnel, and technology, such as the changes cloud computing represents.

The following represents the CIO's high-level update to the strategy, indicating Information Services expectations to accomplish the following according to their established timelines:

1. Build out the security enclave that will allow NARA to add systems and create a single Enterprise Cloud (*this item is contingent upon funding, tentative 12/31/2016*);
2. Educate staff on the Roles and Responsibility matrix as part of the new environment (*October 31, 2016*);
3. Move the systems we have contracted for into the cloud (NAC, DAS, ERA 2.0, WTC) (*NAC, DAS, and ERA 2.0 were completed March 31, 2016. WTC completion expected October 2016*);
4. Evaluate on-premises systems for move to the cloud (*January 2017*);
5. Incorporate cloud into the current governance structure (*completed May 2016*);
6. Finalize Operational procedures for the Cloud (*January 2017*); and
7. Bring on Cloud Engineer (selection was made for a technical expert) (*September 2016*).
8. Finalize plans to implement the 2011 Federal Cloud Computing Strategy (*February 2017*).

### *Risk Assessment for Cloud Computing*

GAO's Green Book provides the overall framework for designing, implementing, and operating an effective control system; and provides updated sections on identifying, assessing, and responding to risks. GAO states management should design control activities to achieve objectives and respond to risks. The recent *Playbook: Enterprise Risk Management for the U.S.*

*Federal Government*, July 29, 2016, aligns with the Green Book and provides a more holistic view of risk management whereby Enterprise Risk Management (ERM) and internal control activities provide risk management support to an agency in different but complementary ways.<sup>10</sup> In order to manage risk effectively, it is important to build strong communication flows and data reporting so employees at all levels in the organization have the information necessary to evaluate and act on risks and opportunities, to share recommendations on ways to improve performance while remaining within acceptable risk thresholds, and to seek input and assistance from across the enterprise. ERM should address the full spectrum of an agency's risk portfolio across all organizational (major units, offices, and lines of business) and business (agency mission, programs, projects, etc.) aspects.

One of the stated objectives of NARA's 2014 Enterprise Cloud Strategy was to manage risks associated with cloud service acquisition, integration, and deployment. However, NARA had not yet conducted a formal exercise to assess the risks associated to its implementation of cloud computing. Risk management activities were ad-hoc. NARA's IT risk management function was overburdened and tasked with identifying and managing risks within its program and project management areas. However, cloud computing was not yet a formally established program within Information Services. Risk Management staff in I's Quality Management Division assisted Project Managers when contemplating moving to the cloud, but it was primarily ad-hoc and there were no formal deliverables associated to the effort.

In addition, we saw that Information Services identified and communicated some risks for the implementation of NARA's Enterprise Cloud contract, which brought some of NARA's disparate infrastructure and platform services under one contract. Though we recognize the benefits of these activities, we also note the level of agency control decreases as services move from IaaS to PaaS to SaaS, and we saw nothing to demonstrate how NARA will more holistically manage those risks.

FedRAMP is beneficial to agencies because it promotes a "do once, use many times" approach, and increases confidence in security assessments. It is estimated to save 30 - 40% of government costs, as well as time and staff required to conduct redundant agency security assessment. NARA's Chief Information Security Officer (CISO) stated NARA had not performed a gap analysis on the risk in not using a FedRAMP certified vendor. The CISO stated a FedRAMP certified vendor is not required. A Branch Chief stated that at the end of the day, NARA still has to ensure FISMA compliance. At a minimum, the Cloud System and CSP must have an ATO from NARA, and NARA recognized there are CSP's which are not FedRAMP certified. NARA's IT contract standards were developed for contractors, which would include CSPs and,

---

<sup>10</sup> ERM includes internal controls but also larger issues of the external environment, as well as transparency, business practices, reporting, and governance that help define the overall risk culture.

the security requirements would be the same to obtain an ATO. We discuss identification of vendor characteristics early in the process in Finding 4.

Our recent audit report also identified weaknesses in NARA's risk management.<sup>11</sup> While NARA appeared to be aware of the significant risks and challenges they faced, the agency had not implemented an ERM program that clearly identified, prioritized, and managed risks throughout the organization. NARA's approach to risks was stove-piped, and risk identification did not span across the enterprise and include risks such as those related to information security. NARA management did not make the implementation of an ERM program a strategic priority. We identified 17 challenges, which included the effectiveness of NARA's Information Security Program. We also identified that NARA offices did not always effectively perform contract monitoring, which creates difficulties for NARA in working effectively with contractors.

Finally, during our field work, we interviewed staff for their opinions on NARA's risks to implementing cloud computing, as seen in [Appendix A](#). The information received highlights the importance of conducting a risk assessment in the area of cloud computing and evaluating actions needed to mitigate associated risks.

Without a formal exercise to fully address the risks associated to cloud computing, NARA will have difficulty building the strong communication flows and data reporting needed so NARA's cloud computing stakeholders have the information necessary to evaluate and act on its risks and opportunities, to share recommendations on ways to improve performance while remaining within acceptable risk thresholds, and to seek input and assistance from across the enterprise. Due to ineffective risk management, NARA experienced difficulties establishing an effective internal control system for its cloud computing program. For example, NARA had difficulties executing its Enterprise Cloud Strategy, establishing a process for an accurate cloud computing inventory, defining and establishing requirements for SLAs, and collecting necessary information for IT investments. These difficulties are discussed later in this report.

## **Recommendations**

We recommend:

**Recommendation 1:** The NARA CIO, 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 document and coordinate activities and establish key control points for NARA's cloud computing program.

---

<sup>11</sup> Audit Report No. 17-AUD-01, *Enterprise-wide Risk Assessment Audit of NARA's Internal Controls*, October 28, 2016



Management Response

NARA concurs with this recommendation. Information Services will implement policies and procedures for acquiring cloud services and Software as a Service (SaaS) offerings, when appropriate.

*Target Completion Date:* December 29, 2017

OIG Analysis

We consider NARA's proposed actions responsive to our report recommendation. However, Information Services should ensure these policies and procedures are developed according to the intent of the recommendation, which would include SaaS as a cloud service, not SaaS in addition to cloud services. The NIST definition of cloud computing states SaaS is one of three cloud computing service.

This recommendation will remain open and resolved, pending completion of the corrective actions identified above.

**Recommendation 2:** The NARA CIO should complete and document a review of existing IT systems for cloud compatibility.

Management Response

NARA concurs with this recommendation. Information Services will evaluate existing systems as part of our normal system evolution process or at the end of contract years for suitable replacements to the cloud.

*Target Completion Date:* December 29, 2017

OIG Analysis

We consider NARA's proposed actions responsive to our report recommendation. However, waiting until the end of a contract year to make such evaluations could leave NARA with inadequate time to select an appropriate vendor. OMBs' Federal Cloud Computing Strategy states successful organizations carefully consider their broad IT portfolios and create roadmaps for cloud deployment and migration, prioritizing services that have high expected value and high readiness to maximize benefits received and minimize deliver risk. Defining exactly which cloud services an organization intends to provide or consume is a fundamental initiation phase activity in developing an agency roadmap. This recommendation will remain open and resolved, pending completion of the corrective actions identified above.

**Recommendation 3:** The NARA CIO should update the Enterprise Cloud Strategy with clearly defined roles and responsibilities, and develop and implement a written plan to execute the strategy.

Management Response

NARA concurs with this recommendation. NARA is currently revising its Enterprise Cloud Strategy. The updated Strategy will include a written plan and will identify roles and responsibilities to execute the cloud strategy.

*Target Completion Date:* December 29, 2017

OIG Analysis

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

**Recommendation 4:** The NARA CIO should conduct and document a risk assessment specific to NARA's implementation of cloud computing in coordination with NARA's Chief Risk Officer.

Management Response

NARA concurs with this recommendation. Information Services will conduct a risk assessment specific to NARA's implementation of cloud computing.

*Target Completion Date:* December 29, 2017

OIG Analysis

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

**Finding 2. NARA lacked an accurate cloud computing inventory.**

NARA maintained several differing inventory listings and had not established an effective method to accurately inventory its cloud computing services. This occurred because NARA lacked a common identifier and designation for its cloud computing services, and the use of a centralized reporting point for those services. As a result, it will be difficult for NARA to apply the controls needed for the unique environment of cloud computing. This will also impair NARA's ability to accurately report performance information related to its cloud computing activities. According to OMB Circular A-130, *Managing Federal Information as a Strategic Resource*, July 28, 2016, agencies shall maintain an inventory of information systems.<sup>12</sup> NIST SP 800-145, *The NIST Definition of Cloud Computing*, September 2011, characterizes the important aspects of cloud computing and is intended to serve as a means for broad comparisons of cloud services and deployment strategies, and to provide a baseline for discussion from what is cloud computing to how to best use cloud computing. The GAO Green Book states monitoring of the internal control system is essential in helping internal control remain aligned with changing objectives, environment, laws, resources, and risks. However, NARA lacked the use of a centralized reporting point for its cloud computing services.

*NARA's Definition of Cloud Computing*

NARA did not standardize and apply its own interpretation of NIST's definition of cloud computing. Business areas with responsibilities for cloud computing relied upon differing terminology, designations and definitions to identify NARA's cloud computing systems. In addition, NARA business areas with cloud computing responsibilities lacked the coordination necessary to practice a centralized approach and develop a common and accurate inventory. As a result, NARA had varying inventories of cloud computing services under different designations, as displayed in the chart below.

---

<sup>12</sup> According to OMB, Maintain an inventory of the agency's major information systems, information holdings, and dissemination products, at the level of detail that OMB and the agency determine is most appropriate for overseeing and managing the information resources; and shall maintain an inventory of the agency's information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII to allow the agency to regularly review its PII and ensure, to the extent reasonably practicable, that such PII is accurate, relevant, timely, and complete; and to allow the agency to reduce its PII to the minimum necessary for the proper performance of authorized agency function.

**NARA Sources of Cloud Computing Inventory**

<b>Inventory Source</b>	<b>Designation Used</b>	<b>Count</b>
<b>NARA Enterprise Cloud Strategy, July 22, 2014</b>	Existing Cloud and IT Service-Based Implementations	19
<b>Cloud Program Manager, October 14, 2015</b>	IaaS and PaaS Contracts	7
<b>Cloud Program Manager, December 15, 2015</b>	Existing IaaS and PaaS Contracts	10
<b>IT Security, July 2016</b>	Cloud Inventory for IT Security Lead's Purposes	8
<b>CPIC OMB A11 Reporting, FY 2016</b>	Provisioned IT Services	18
<b>CPIC FedRAMP Reporting - eGov Integrated Data Collection, FY 2015</b>	FedRAMP	15
<b>CPIC Investment Tracker, FY 2016</b>	No designation of cloud services	25
<b>Acquisitions Contracts, July 2016</b>	No designation of cloud services	73
<b>NARA FISMA Master Listing &amp; OIG Survey, May 2016</b>	Total contractor and cloud systems	8

We observed gaps, errors, and inconsistencies in the number of cloud computing services reported by NARA business areas. For example, in FY 2014 NARA acquired a Software as a Service solution, OpsPlanner, for emergency planning, alert notification and incident planning, however this service was not included in any of the inventories. CPIC maintained at least three different inventories for external reporting reasons. In addition, NARA did not consistently report cloud computing services. NARA also included cloud systems such as Google Apps and Internal Collaboration Network in its FY 2015 Master FISMA reportable inventory, NARA's most comprehensive listing of all IT systems.<sup>13</sup> However, NARA then dropped these systems from its FY 2016 FISMA Inventory. We found further inconsistencies in CPIC's IT Portfolio for provisioned services, which also excluded Google Apps for FY 2016 and FY 2017.

In addition, we received two different inventory lists from the Program Manager responsible for cloud computing at NARA, yet these lists were limited to IaaS and PaaS contracts. One contained seven contracts and was reported to have been generated by Acquisitions, while the other listing contained ten contracts and was part of a briefing to senior management. The Program Manager told us Acquisitions provides the inventories for all cloud computing services. However, when we received an inventory listing from the Acquisitions CO responsible for IT contracts, it comprised 73 IT contracts with no designations for whether or not they were cloud computing services, or for the types of services that might exist, such as IaaS, PaaS, and SaaS. When we asked the responsible Acquisition CO to identify SaaS contracts for purposes of

---

<sup>13</sup> During the Audit of NARA's Information Systems Inventory, 17-AUD-02, we identified shortcomings in NARA's system inventory process. Though NARA had a master FISMA reportable inventory, they lacked a comprehensive inventory of all NARA information systems. In response to the audit, NARA is developing a process for conducting a comprehensive official systems inventory, which will include FISMA reportable systems.

monitoring SLAs, the Acquisitions staff member was unable to do so and deferred us to other business areas in Information Services.

We also observed basic naming conventions, descriptions of systems, and field lengths were inconsistent among the varying inventories, for example, terms for NARA's mail service. terms "Google" and "Google Apps for Government," (the FY 2015 FISMA Listing used the terms "Google" and "NARA Google Apps/Cloud Email," and the Acquisitions listing used the term "cloud mail." These inconsistencies create further impediments to reconciling the inventory information. A consistent data dictionary could be helpful.

Upon our initial inquiry, Information Services stated they relied upon the NIST definition of cloud computing.<sup>14</sup> We also found both the NARA Enterprise Cloud Strategy and NARA's draft *Standard IT Security Contractual Requirements for Unclassified Information/Information Systems* used the NIST definition of cloud computing. However, NIST's definition of cloud computing is broad. According to NIST, its definition characterizes the important aspects of cloud computing and is intended to serve as a means for broad comparisons of cloud services and deployment strategies, and to provide a baseline for discussion from what is cloud computing to how to best use cloud computing. We found nothing to demonstrate NARA held the conversations necessary to determine how the agency would build upon NIST's definition and create the level of specificity necessary to achieve a standard application of the NIST definition. Further emphasizing the need for standardization, some inventories relied upon additional definitions, such as "provisioned IT services", for reporting purposes. These additional terms are listed in [Appendix B](#).

In order to understand how NARA applied the definition of cloud computing, we acquired internal terminology used by NARA staff with varying responsibilities for cloud computing activities, including the Capital Planning Program Manager, the IT Risk Manager, the Deputy CIO, the Cloud Program Manager, and the Branch Chief for IT Security Support. We also reviewed NARA's written guidance ([Appendix B](#)), as well as federal requirements and guidance ([Appendix C](#)), and found a lack of consistency in NARA's application of the definition of cloud computing.

---

<sup>14</sup> SP 800-145, *The NIST Definition of Cloud Computing*, September 2011, states: Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models. Essential characteristics include on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. Service models include Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Cloud services can be deployed through private, community, public, or hybrid clouds.

Each NARA representative brought forth a unique perspective on the application of cloud computing. For example, NARA representative 1 used the OMB definition, which is basically if it's not at NARA, it's cloud, and stated there was a change in the definition used in OMB Circular A-11, when they changed the language from cloud spending to provisioned services, and they now also have provisioned non-cloud. The same respondent also indicated not all provisioned services are cloud environments because they may be NARA systems that are on dedicated servers, such as OAS, or services that NARA uses from other Federal agencies that are not NARA systems and in which case NARA does not believe they are cloud environments. Representative 2's understanding of the application of cloud computing was if NARA does not have direct responsibility for managing and hosting; it's not on premise. Representative 3 stated if it's a hosted system and one can go to the data center and watch it, play with it, touch the hardware, then it's not cloud. If one cannot do that, then it's cloud.

Representative 4 replied they base what is and is not cloud on whether or not it's hosted externally in a FedRAMP environment, and this is designated in the Business Case Form. Representative 5 believed there were a lot of things going into whether or not something was a cloud system. It has to be evaluated for things such as sensitive information which would need protections and could not be provided in a cloud, or the length of the contract. For example, if it's only a few months term, it might be more efficient to keep it at NARA. Those things are evaluated through the business case. Representative 6 believed if it's not at NARA, it's in the cloud. Anything that's not managed by NARA, the security requirements are the same. The representative added they all have to meet NARA requirements to maintain security according to FISMA, NARA 804, and NIST. And, whether or not the contractor goes through FedRAMP, it does not really matter from a security standpoint.

We observed nothing in NARA's internal written guidance which demonstrated a consistent application of cloud computing or which standardized the terminology used in identification and designation of cloud computing services at NARA, as seen in [Appendix B](#). Further, OIG recently conducted an information system inventory at NARA, which used additional terminology to identify and designate these types of services.<sup>15</sup> For example, contractor; third-party; contractor and cloud; third-party and cloud; and contractor, cloud or third-party.

NARA's internal guidance and staff members' interpretations of cloud computing, coupled with the greater federal designations and best practices, emphasize the need to build upon the baseline definition established by NIST so that NARA can establish a standard application of the definition of cloud computing. Developing a centralized reporting mechanism will enable NARA to apply the controls needed to oversee the unique aspects of cloud computing.

---

<sup>15</sup> Audit Report No. 17-AUD-02, *Audit of NARA's Information System Inventory*, November 4, 2016.

## **Recommendations**

We recommend:

**Recommendation 5:** The NARA CIO should develop, approve, and implement written NARA-wide standardized criteria, terms, and definitions to distinguish its cloud computing services from other IT services; and verify those standards are used for the early identification and designation of cloud computing services.

### Management Response

NARA concurs with this recommendation. NARA will develop standardized terms and definitions for cloud computing services.

*Target Completion Date:* December 29, 2017

### OIG Analysis

We consider NARA's proposed actions responsive to our report recommendation. However, as with all corrective actions in this report, NARA should ensure their approval and implementation. This recommendation will remain open and resolved, pending completion of the corrective actions identified above.

**Recommendation 6:** The NARA 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.

### Management Response

NARA concurs with this recommendation. NARA will identify a centralized reporting point and written process for tracking cloud systems, system owners and business areas within its system inventory document.

*Target Completion Date:* December 29, 2017

### OIG Analysis

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

**Finding 3. NARA executed cloud contracts without established standards in place.**

Despite years of implementing cloud computing contracts, NARA did not yet have an approved requirement to include a common set of procedures for CSPs to follow, including expected levels of service, as part of its cloud computing contracts. No reviews were conducted to determine the extent of contracts that may be without SLAs. In addition, NARA's approach to monitoring lacked policies and procedures for a centralized monitoring method for its SLAs and lacked a central location for maintaining associated reports. Further, NARA was executing its cloud computing contracts without approved standards for contractual language. Although NARA developed draft standards for IT contractual language in April 2016, the agency did not develop the standards according to a plan which clearly included considerations for existing guidance and best practices available. NARA did not consider development of cloud provisioning guidelines a priority, which may have impaired its ability to establish effective controls and monitor service levels of cloud computing contracts. As a result, NARA may not be able to consistently and accurately measure the performance levels of NARA's cloud computing contracts in order to achieve the full benefits of a "Cloud First" policy.

CIOC/CAOC Best Practices state SLAs are agreements under the umbrella of the overall cloud computing contract between a CSP and a federal agency, which define acceptable service levels to be provided by the CSP to its customers in measurable terms. The definition, measurement and enforcement of the performance parameters specified in SLAs varies widely among CSPs. Therefore, Federal agencies should ensure that CSP performance is clearly specified in all SLAs and that all such agreements are fully incorporated, either by full text or by reference, into the CSP contract. NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013, states the level of control is usually established by the terms and conditions of the contracts or service-level agreements with the external service providers, and can range from extensive control to very limited control. Organizations need to document the basis for trust relationships so the relationships can be monitored over time.

When federal agencies place federal data in a CSP environment, they are inherently giving up control over certain aspects of the services they consume. Agencies should enforce SLA performance by requiring in the reporting clauses of the SLA and the contract that CSPs submit reports or provide a dashboard where Federal agencies can continuously verify that service levels are being met. When procuring and managing service contracts for cloud services and other IT services, it is important to specify security requirements upfront but it is even more important to



be able to monitor and verify whether these security requirements are being met throughout the lifetime of the contract.<sup>16</sup>

*NARA Standards for IT Contracts*

Though NARA was late in developing its own standards for requirements in IT contracts, considerable guidance had become available in the more than 5 years since OMB instituted its “Cloud First” policy in 2010. For example:

- NIST SP 800-144 *Guidelines on Security and Privacy in Public Cloud Computing*, December 2011;
- CIOC/CAOC *Creating Effective Cloud Computing Contracts for the Federal Government, Best Practices for Acquiring IT as a Service*, February 24, 2012;
- NIST SP 500-291, *NIST Cloud Computing Standards Roadmap*, Version 2, July 2013
- GSA Whitepaper *Best Practices for Effective Cloud Computing Services Procurement within the Federal Government*, January 2016;
- Appropriate FAR Clauses such as 52.204–21, Basic Safeguarding of Covered Contractor Information Systems, June 2016; and
- FedRAMP *Control Specific Contract Clauses*, Version 2, June 6, 2014.

We obtained and reviewed NARA’s draft *Standard IT Security Contractual Requirements*, April 18, 2016, to determine if NARA considered and incorporated some of the elements from the above mentioned cloud computing guidance. Our review found gaps, for example:

- The standards did not require an SLA or similar mechanism to define performance with clear terms and definitions, demonstrating how performance would be measured, and what enforcement mechanisms would be in place to ensure terms were met;
- The standards did not require a mechanism to describe how uptime would be calculated;
- The standards did not require the provider to notify NARA of changes to terms of service if the provider reserves the right to modify the terms of the service agreement at any time;
- The standards did not require including comprehensive FAR clauses, such as 52.204-21, Basic Safeguarding of Covered Contractor Information Systems, June 2016; and
- The standards did not include methods to monitor the service level providers to ensure SLAs were met.

When we inquired as to how the standards were developed, we determined that a new NARA staff member in Information Services developed the standards within about a month of arrival, later adding the CISO assisted. At the time of our inquiry, the staff member stated the standards were not developed according to any written plan and were under review by NARA’s General Counsel (NGC). The standards were stated to have been presented to Acquisitions afterward.

---

<sup>16</sup> European Network and Information Security Agency (ENISA) *Procure Secure A guide to monitoring of security service levels in cloud contracts*, April 2, 2012

The CISO stated Capital Planning was not involved in developing the standards. After our inquiries, Information Services reported meeting with both Acquisitions and NGC, and NGC was still reviewing as of October 2016, and the standards were still in draft as of November 2016.

Without a written plan to develop the standards, we found NARA made ad-hoc considerations for available guidance when developing the standards. Information Services officials confirmed there was no written plan used to develop the standards. Instead, NARA relied heavily on benchmarking with another federal agency. Though we believe benchmarking to be a prudent activity, collaboration with business areas and consideration for available standards should have been at the forefront of NARA's approach to planning its development of the standards.

Some of the delay in establishing these standards can be attributed to NARA improperly planning out its prioritization of tasks in the *NARA Enterprise Architecture FY 2015 Agency Enterprise Roadmap, Version 2, May 18, 2015*. According to the Roadmap, to "develop cloud provisioning guidelines" was 15<sup>th</sup> of 19 priorities. NARA acknowledged that inconsistent and project focused deployments of cloud services could increase costs, increase integration complexity, duplicate acquisition and SLA management efforts, or increase costs. However, the development of provisioning guidelines did not receive priority. Initially, the Deputy CIO and Cloud Program Manager separately stated cloud provisioning guidelines were being developed. The Deputy CIO later stated in lieu of "Cloud Provisioning Guidelines" they created a prioritized list of projects to be moved to the cloud, and an SOP for migrating systems to the cloud. The latter document contained a section on "Cloud Migration Assessment" which serves as Provisioning Guidelines at the design level. Provisioning guidelines at the operational level would belong to Ops and InfoReliance.

We did not obtain and review the SOP referred to, but note that according to OMB's *Federal Cloud Computing Strategy*, February 8, 2011, in order to effectively provision selected IT services, agencies will need to rethink their processes as provisioning services rather than simply contracting assets. Contracts that previously focused on metrics such as number of servers and network bandwidth now should focus on the quality of service fulfillment. Organizations that are most successful in cloud service provisioning carefully think through a number of factors including: 1) aggregate demand, 2) integrate services, 3) contract effectively, and 4) realize value. Though we believe NARA exercised some of these factors with its Enterprise Cloud Contract, the agency will have to make broader considerations for establishing provisioning guidelines which are more in line with the provisioning framework in OMB's strategy and focus on the quality of service fulfillment. For example, establishing effective standards for cloud computing contracts.

*Monitoring of Service Levels*

NIST states SLAs can be pre-defined or negotiable and define expectations of performance for security controls, describe measurable outcomes, and identify remedies and response requirements for identified instances of noncompliance in the event the provider fails to deliver the service at the level specified.

NARA did not have a mechanism for centralized monitoring of service levels in cloud computing contracts. NARA 101, Part 14.e, October 2, 2016, requires Acquisitions to develop a program for routine evaluation of contract performance. When we asked about monthly reports for monitoring service levels, IT Operations told us CORs monitor the service levels. The Acquisitions CO responsible for all IT contracts confirmed monitoring service levels for SaaS was done by Acquisitions, and primarily achieved through email. We observed that Acquisitions monitors service levels for SaaS, and Information Services monitors service levels for IaaS and PaaS. The Acquisitions Director confirmed these responsibilities were delegated to the CORs. However, the Acquisitions Director also stated Acquisitions did not monitor contractor performance and this was a program function.

The Acquisitions CO first thought service level reports might be maintained on the agency shared drive, however the CO was unable to demonstrate the location and said the reports were maintained in email. The Acquisitions CO is cc'd on the reports the CORs receive via email, and also notified of issues via email. The Acquisitions CO was unable to point to any specific software contracts being monitored by Acquisitions during our initial meeting, and subsequently provided documentation which showed NARA's receipt of monthly monitoring of service levels for a cloud contract. In addition, we were provided a monthly management report and learned they did not track staffing levels in at least one operations and maintenance contract.

Within IT Operations, we spoke with the COR for NARA's Enterprise Cloud contract and found a different method of monitoring. Though we received documentation to support the COR was responsible for the SLAs, this COR did not directly monitor the associated SLAs because those responsibilities were delegated to the System Owners who received the reports and only reported back to the COR when there were issues. However, the COR acknowledged the System Owners were often not prepared to deal with those responsibilities. In addition, at the time of our request, the COR was aware the IaaS contractor was a few months behind on providing service level reports to NARA.

Contributing to this condition, the Acquisitions CO was not aware of any documented standards NARA might have regarding monitoring SLAs. The Deputy CIO stated this documentation was still in development, and IT Operations was finalizing metrics for NARA's SLA standards. When we then spoke with IT Operations staff, we learned a roles and responsibilities matrix for monitoring security aspects of contracts for the Enterprise Cloud Contract was under

development and would include tasks such as monitoring access control lists (ACL). Information Services expected to use the Responsible, Accountable, Consulted, and/or Informed (RACI) chart as a standard that could be applied to other contracts going forward. According to RACI assignments for capacity and performance monitoring, the System Owner was accountable and the contractor, InfoReliance, was responsible, while the CORs were among the informed. We acknowledge RACI charts as useful tools for defining responsibilities for processes, and identification of who is responsible, accountable, consulted and informed.<sup>17</sup> However, NARA's RACI was specific to the Enterprise Cloud Contract and provided no details of the processes described nor any associated standards for monitoring, such as how NARA will perform capacity and performance monitoring, and management of ACLs.

Mentioned prior in this report, NARA's draft *Cloud Security Architecture Reference*, March 2013, contained a section for specific cloud monitoring considerations by layer, cautioning "trust in providers should not be blind, and should be codified in the SLA and verified with regular, frequent status reports," and "lines of responsibility should be clear in any SLA." However, the document did not further provide or reference specific expectations for SLAs, such as the frequency of status reports, or a standard monitoring process.

We note existing best practices suggest monitoring parameters for SLAs should be selected according to use-case (e.g. IaaS, PaaS, and SaaS have different monitoring requirements and/or division of responsibilities), and be based on an analysis of an organization's principal areas of risk and impact that the IT service will have on these.<sup>18</sup> Further, metrics applicable to managed services that can be used as SLAs include service level objectives (SLOs) such as the Recovery Point Objective (RPO) and Recovery Time Objective (RTO). These often apply to application and service hosting scenarios. In relation to SLAs, it is also important to understand and define the terms of conditions, measures – including definitions for any measurements and related calculations, and enforcement mechanisms.<sup>19</sup>

#### *Review of Existing Contracts for Service Level Agreements*

We also found NARA may have existing cloud computing contracts without SLAs. When we asked the Acquisitions CO responsible for NARA's IT contracts about SLAs, the manager referred to a recent experience dealing with a contract that lacked a service level agreement. The manager stated it was very difficult and took nearly one year to establish a SLA. When we inquired as to whether or not NARA has reviewed existing contracts for SLAs, the Acquisitions

---

<sup>17</sup> ISACA Presentation *COBIT Transforming Enterprise IT*, 2009

<sup>18</sup> European Network and Information Security Agency (ENISA) *Procure Secure A guide to monitoring of security service levels in cloud contracts*, April 2, 2012

<sup>19</sup> GSA Whitepaper *Best Practices for Effective Cloud Computing Services Procurement within the Federal Government*, January 2016

CO stated it would take time to do such a review, and there were not enough resources. During another recent audit, we observed similar resource limitations in the Contract Oversight Branch, established in 2011 to assist with duties such as evaluating contractor performance, where the office had been vacant since inception.<sup>20</sup> In July 2016, the Acquisitions Director reported they were not likely to ever fill the position in Contractor Oversight. By November 2016, the Director reported hiring an IT Acquisitions Liaison, while expecting to re-advertise for an additional staff member. We plan to address this risk by evaluating contracts and SLAs through a separate audit.

## **Recommendations**

We recommend:

**Recommendation 7:** The NARA CIO should coordinate with necessary business areas including Acquisitions and General Counsel to develop, approve, and implement its written cloud provisioning guidelines.

### Management Response

NARA concurs with this recommendation. NARA will develop cloud provisioning guidelines.

*Target Completion Date:* December 29, 2017

### OIG Analysis

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

**Recommendation 8:** The NARA 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.

### Management Response

NARA concurs with this recommendation. NARA will update its standard contract language to include security requirements for cloud systems.

*Target Completion Date:* December 29, 2017

---

<sup>20</sup> Audit Report No. 17-AUD-06, *Audit of NARA's Procurement Program*, November 15, 2016

OIG Analysis

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

**Recommendation 9:** The NARA 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.

Management Response

NARA concurs with this recommendation. NARA will develop appropriate procedures for monitoring Service Level Agreements.

*Target Completion Date:* December 29, 2017

OIG Analysis

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

#### **Finding 4. CPIC's Business Case Form could be improved.**

We determined the design and content of CPIC's Business Case form did not allow for consistent and comprehensive collection of information needed for proposed IT investments. This occurred because CPIC did not incorporate relevant guidance and best practices for IT acquisitions into the content of the form. The form used lacked formal approval and was part of a temporary directive for interim guidance from FY 2012, NARA 801-3, *Temporary Capital Planning and Investment Control Process*, September 17, 2014. As a result, CPIC's Business Case Form was not as effective as it could be at capturing beneficial information on NARA's cloud computing activities. This may impair NARA's ability to make decisions which ensure IT projects align with NARA's mission and strategic goals. Further, NARA may not be fully considering the benefits of FedRAMP's "do once, use many times" approach.

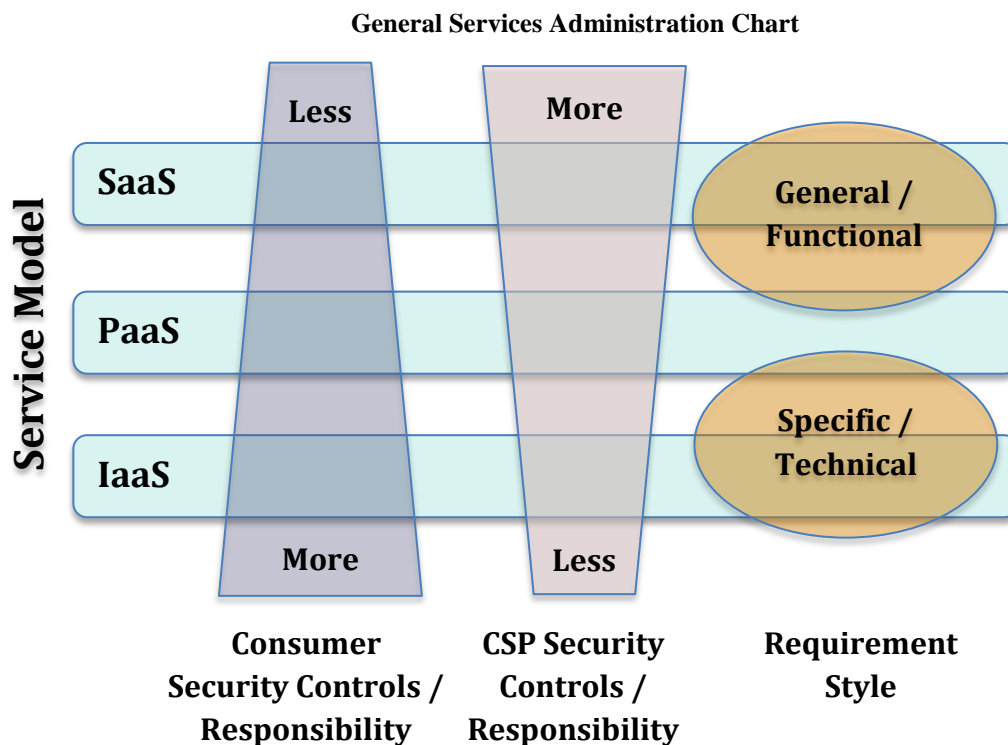
The General Services Administration (GSA) Whitepaper, *Best Practices for Cloud Computing Services Procurement within the Federal Government*, January 2016, provides useful information to assist in the development of standards for cloud computing services procurement. The whitepaper states an important consideration for cloud procurement is planning from the very beginning for how the contract will terminate and services will be moved to another vendor. Some important elements to capture:

- Responsibilities of primary business unit and participating business units;
- Whether or not a vendor is FedRAMP compliant;
- The type of service being considered (infrastructure, platform, software);
- Whether or not there may be an existing/legacy system being replaced; and
- Assignment of a contracting officer early on.

NARA's Business Case form could capture additional information to improve the cloud computing process. For example, the form does not capture whether an investment is a contractor system, externally hosted, on-premises, off-premises, or whether a vendor is FedRAMP certified. Further, in the event a vendor is not FedRAMP certified, the form does not require gathering information on whether the contractor may grant the appropriate access for NARA to conduct its own security assessment for an ATO. Our review of NARA's forms demonstrated some respondents voluntarily indicated when a vendor was FedRAMP compliant. NARA's draft standards for IT contracts acknowledge not all CSPs may be FedRAMP certified and NARA may have to conduct its own security assessment for an ATO. Collecting this information early on would allow NARA to identify and better prepare for such situations.

Additionally, NARA's form does not capture the type of cloud service being considered, such as IaaS, PaaS, or SaaS. GSA's graph highlights the importance of the type of service being considered, since the amount of customer control varies with each type of service offering. Each

cloud service model presents unique functionality with agency security controls and responsibilities decreasing as you move from infrastructure to platform to software. GSA illustrated the levels of controls within the following diagram.



The form also did not capture key information such as service level requirements, Continuity of Operations (COOP) requirements, the business unit submitting the proposal, participating business units, whether or not there's an existing system, or whether or not a legacy system is being replaced, a best practices recommendation. In addition, the form does not require approval sign off of the responsible business unit executive. More comprehensive capture of information on the CPIC Business Form will improve capital planning and increase the likelihood NARA will realize the full benefits of cloud computing.

**Recommendations**

We recommend:

**Recommendation 10:** The NARA CIO should coordinate with the Chief Acquisition 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.



Management Response

NARA concurs with this recommendation. Once NARA addresses other relevant recommendations from this audit – including issuing an updated Cloud Strategy, developing standardized terms, and issuing cloud provisioning guidelines – NARA will review CPIC policies and deliverables to ensure NARA cloud strategy is appropriately addressed in capital planning processes.

*Target Completion Date:* June 30, 2018

OIG Analysis

We consider NARA’s proposed actions responsive to our report recommendation. CPIC’s Business Case Form is critical to the IRB in making decisions regarding selection of IT. Improving the quality of information for the IRB’s decisions is essential for NARA’s governance process. This recommendation will remain open and resolved, pending completion of the corrective actions identified above.

## Appendix A – NARA Identified Cloud Computing Risks

---

NARA Staff Members	Cloud Computing Risks Identified
Respondent 1	One of NARA's greatest risks is in their current contracting vehicle because the way it's set up will require modifications as new things are added.
Respondent 2	NARA's "challenge" is deciding what to do with legacy systems. NARA's acquisition challenge is identifying roles and responsibilities of program offices. Details must be laid out in Service Level Agreements.
Respondent 3	Believes the greatest risk to NARA's implementation of cloud computing is the communications – how are they making sure customers know what the cloud is, how NARA can assist them, allowing them to leverage the cloud and having vendors under one roof versus disparate vendors.
Respondent 4	Believes awarding the ECC has been helpful, as is the IT Security Architecture document because the architecture document outlines the way it should be implemented (in a prior conversation, the respondent stated this was in draft and specific to the Enterprise Cloud Contract). Some basic standard services need to be established in terms of monitoring, and that is where the Enterprise Cloud Contract will help. Believes the cloud security architecture is the way to go, and the continuous authorization of those services.
Respondent 5	Believes the agency is using a tactical mode versus a strategic mode. Instead of picking pieces to put in the cloud, the agency should evaluate everything for cloud consideration.
Respondent 6	Risk assessments in this area involve those performed as part of the security assessment process. However, SOWs are also assessed for risks.
Respondent 7	Greatest concern is acquisitions. Many clouds are based on a utility model, paying for services as needed, so it's very difficult to predict the costs over the period of a contract. NARA's needs changes frequently, for example, the influx of a President's records can be very costly.
Respondent 8	Believed not doing the cost benefit analysis to be the greatest risk.

Respondent 9	Believed that even at this late date, they didn't know whether everyone had the same interpretation of the implementation of cloud computing for the agency.
Respondent 10	Stated NARA is way too late in getting a person in Operations who understands the new model of cloud computing and can drive this. They've posted for someone, but that should have been done a year ago. Regarding NARA's immaturity regarding cloud computing activities, it's not for a lack of strategic thinking; the issues are 100% a lack of resources, and then problems with Acquisitions to get contracts out and get jobs posted. Acknowledged the large amount of vacancies in various I positions, as well as confusion with roles and responsibilities.
Respondent 11	Stated that though it's great they have the Enterprise Cloud Contract, there is risk of time delays in getting the agency up to speed. Some services will be slow to move to the cloud because each service requires a new task order. And, the agency may be dangerously close to the dollar cap on the Enterprise Cloud Contract due to the large amounts of data in the DAS and Catalogue contracts. So, while waiting for Information Services to provide a process to move things to the cloud, there's definitely a risk to timeliness.
Respondent 12	Believes that the risk is in the unknown vulnerabilities – you're getting it out to the cloud, but getting it back can be difficult.
Respondent 13	Believes NARA's greatest risk is in the collaboration between division lines. Many roles and responsibilities are as yet undefined, resulting in confusion and tension.
Respondent 14	Cloud security services varied from provider to provider.

## Appendix B – Examples of Internal Definitions and Designations of Cloud Computing at NARA

---

Title/Date	NARA Internal Cloud Computing Interpretations
NARA Enterprise Cloud Strategy, July 2014	Relies on the terms in the NIST definition of cloud computing.
NARA Draft Standard IT Security Contractual Requirements, April 18, 2016	Relies on the terms in the NIST Definition of Cloud Computing."
NARA IT Security Methodology for C&A and Security Assessments, April, 20, 2016	Uses the terms “external information system service,” and “external service providers.” Further defines “cloud computing” and a “cloud system.”
NARA's Master System List, April 2016	Uses OMB’s term, Provisioned IT Services – An IT service that is owned, operated, and provided by an outside vendor or external government organization and consumed by the agency on an as-needed basis.

## Appendix C – Examples of External Terminology, Definitions and Designations of Cloud Computing

Title	Federal Cloud Computing Terminology
<p>NIST SP 800-145 <i>The NIST Definition of Cloud Computing</i>, September 2011</p>	<p>Purpose and Scope: Cloud computing is an evolving paradigm. The NIST definition characterizes important aspects of cloud computing and is intended to serve as a means for broad comparisons of cloud services and deployment strategies, and to provide a baseline for discussion from what is cloud computing to how to best use cloud computing. The service and deployment models defined form a simple taxonomy that is not intended to prescribe or constrain any particular method of deployment, service delivery, or business operation.</p> <p>Definition: Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. ...</p> <p>Service models include Infrastructure as a Service (IaaS), Platform as a Service, (PaaS) and Software as a Service (SaaS).</p>
<p>NIST SP 800-53 Rev4, <i>Security &amp; Privacy Controls for Federal Information Systems and Organizations</i>, April 2013</p>	<p>Uses the term “external information system services.” Organizations are becoming increasingly reliant on information system services provided by external providers to conduct important missions and business functions. External information system services are computing and information technology services implemented outside of the traditional security authorization boundaries established by organizations for their information systems. Those traditional authorization boundaries linked to physical space and control of assets, are being extended (both physically and logically) with the growing use of external services. In this context, external services can be provided by: (i) entities within the organization but outside of the security authorization boundaries established for organizational information systems; (ii) entities outside of the organization either in the public sector (e.g., federal agencies) or private sector (e.g., commercial service providers); or (iii) some combination of the public and private sector options. External information system services include, for example, the use of service-oriented architectures (SOAs), cloud-based services (infrastructure, platform, software), or data center operations. External information system services may be used by, but are typically not part of, organizational information systems. In some situations, external information system services may completely</p>

	replace or heavily augment the routine functionality of internal organizational information systems.
OMB Circular A-130, <i>Managing Information as a Strategic Resource</i> , July 28, 2016	Uses the term “Provisioned IT Service,” which means an IT service that is owned, operated, and provided by an outside vendor or external government organization, and consumed by the agency on an as-needed basis.
ISO/IEC 17788:2014 <i>Cloud Computing Overview &amp; Vocabulary</i>	Uses the term “cloud computing,” which is a paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.
FAR 52.204-21 <i>Basic Safeguarding of Covered Contractor Information Systems and Organizations</i> , June 2016	Uses the term "covered contractor information system," which means an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information."
FY 2016 <i>Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics</i> , September 26, 2016	Uses the term “contractor operated systems.” Asks whether the agency identifies and maintains an up-to-date system inventory, including organization- and contractor-operated systems, hosting environments, and systems residing in the public, hybrid, or private cloud.

## **Appendix D – Potential Future Audit Work**

---

As a result of this audit, we identified issues which may result in future audit work.

- Review of cloud computing contracts to determine whether or not NARA includes necessary contractual language and FAR clauses according to federal requirements and guidance.
- Review of incident response capabilities within contractor hosted external environments to determine whether adequate controls are in place to manage an information security compromise.

## Appendix E – Acronyms

---

ACL	Access Control List
ARB	Architecture Review Board
ATO	Authorization to Operate
BCN	Business Support Services
BNRB	Business Need Review Board
CPIC	Capital Planning and Investment Control
CAOC	Chief Acquisition Officers Council
CIOC	Chief Information Officers Council
CISO	Chief Information Security Officer
CO	Contracting Officer
COOP	Continuity of Operations
COR	Contracting Officer Representative
CSP	Cloud Service Provider
ENISA	European Network and Information Security Agency
ERM	Enterprise Risk Management
FAR	Federal Acquisition Regulation
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Modernization Act
FOIA	Freedom of Information Act
GAO	Government Accountability Office
GSA	General Services Administration
ISSC	Information Systems Steering Committee
I	Information Services
IT	Information Technology
IaaS	Infrastructure as a Service
NARA	National Archives & Records Administration
NGC	General Counsel
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PaaS	Platform as a Service
RACI	Responsible, Accountable, Consulted, and/or Informed
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SLA	Service Level Agreement
SaaS	Software as a Service
SDLC	System Development Life Cycle
SLO	Service Level Objectives
SME	Subject Matter Expert



## Appendix F – Management Response

---



Date: MAR 09 2017  
To: James Springs, Inspector General  
From: David S. Ferriero, Archivist of the United States  
Subject: Management's Response to OIG Report 17-AUD-08, *NARA's Adoption and Management of Cloud Computing*

We appreciate the efforts of your staff in the subject audit report. Attached is our action plan for the ten recommendations. As each recommendation is satisfied, we will provide documentation to your office.

If you have questions about this action plan or the documentation, please contact Kimm Richards at [kimm.richards@nara.gov](mailto:kimm.richards@nara.gov) or by phone at 301-837-1668.



DAVID S. FERRIERO  
Archivist of the United States

Attachment

NATIONAL ARCHIVES *and*  
RECORDS ADMINISTRATION  
8601 ADELPHI ROAD  
COLLEGE PARK, MD 20740-6001  
[www.archives.gov](http://www.archives.gov)

**Action Plan Response to OIG Report:  
17-AUD-08, *NARA's Adoption and Management of Cloud Computing***

**Recommendation 1:** The NARA CIO, 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 document and coordinate activities and establish key control points for NARA's cloud computing program.

**Planned Action:** Information Services will implement policies and procedures for acquiring cloud services and Software as a Service (SaaS) offerings, when appropriate.

**Target Completion Date:** December 29, 2017

**Recommendation 2:** The NARA CIO should complete and document a review of existing IT systems for cloud compatibility.

**Planned Action:** Information Services will evaluate existing systems as part of our normal system evolution process or at the end of contract years for suitable replacements to the cloud.

**Target Completion Date:** December 29, 2017

**Recommendation 3:** The NARA CIO should update the Enterprise Cloud Strategy with clearly defined roles and responsibilities, and develop and implement a written plan to execute the strategy.

**Planned Action:** NARA is currently revising its Enterprise Cloud Strategy. The updated Strategy will include a written plan and will identify roles and responsibilities to execute the cloud strategy.

**Target Completion Date:** December 29, 2017

**Recommendation 4:** The NARA CIO should conduct and document a risk assessment specific to NARA's implementation of cloud computing in coordination with NARA's Chief Risk Officer.

**Planned Action:** Information Services will conduct a risk assessment specific to NARA's implementation of cloud computing.

**Target Completion Date:** December 29, 2017

**Recommendation 5:** The NARA CIO should develop, approve, and implement NARA-wide standardized criteria, terms and definitions to distinguish its cloud computing services from other IT services; and verify those standards are used for the early identification and ongoing designation of cloud computing services.

**Planned Action:** NARA will develop standardized terms and definitions for cloud computing services.

**Target Completion Date:** December 29, 2017

**Recommendation 6:** The NARA 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.

**Planned Action:** NARA will identify a centralized reporting point and written process for tracking cloud systems, system owners, and business areas within its system inventory document.

**Target Completion Date:** December 29, 2017

**Recommendation 7:** The NARA CIO should coordinate with necessary business areas including Acquisitions and General Counsel to develop, approve, and implement its written cloud provisioning guidelines.

**Planned Action:** NARA will develop cloud provisioning guidelines.

**Target Completion Date:** December 29, 2017

**Recommendation 8:** The NARA 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.

**Planned Action:** NARA will update its standard contract language to include security requirements for cloud systems.

**Target Completion Date:** December 29, 2017

**Recommendation 9:** The NARA 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.

**Planned Action:** NARA will develop appropriate procedures for monitoring Service Level Agreements.

**Target Completion Date:** December 29, 2017

**Recommendation 10:** The NARA CIO should coordinate with the Chief Acquisition 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.

**Planned Action:** Once NARA addresses other relevant recommendations from this audit – including issuing an updated Cloud Strategy, developing standardized terms, and issuing cloud provisioning guidelines – NARA will review CPIC policies and deliverables to ensure NARA cloud strategy is appropriately addressed in capital planning processes.

**Target Completion Date:** June 30, 2018

## Appendix G – Report Distribution List

---

Archivist of the United States  
Deputy Archivist of the United States  
Chief Operating Officer  
Deputy Chief Operating Officer  
Chief of Management and Administration  
Chief Information Officer  
Deputy Chief Information Officer  
Chief Acquisition Officer  
Office of General Counsel  
Accountability  
United States House Committee on Oversight and Government Reform  
Senate Homeland Security and Governmental Affairs Committee

## OIG Hotline

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

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

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

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