




Inspector General

September 30, 2024

TO: Dr. Colleen Shogan
Archivist of the United States

FROM: Dr. Brett M. Baker
Inspector General 

SUBJECT: *Audit of NARA's Cloud Computing Services*
OIG Audit Report No. 24-AUD-09

The Office of Inspector General (OIG) contracted with Sikich CPA LLC (Sikich) to conduct an independent performance audit of NARA's Cloud Computing Services. Attached is Sikich's report titled Performance Audit of NARA's Cloud Computing Services. The objective of this audit was to assess NARA's efforts relating to cloud computing management. Specifically, the audit examined whether NARA has effectively implemented plans and procedures to meet federal requirements. The report contains four recommendations that are intended to strengthen NARA's management of its cloud computing environment. Agency staff indicated they had no comments for inclusion in this report.

Sikich is responsible for the attached auditor's report dated September 27, 2024 and the conclusions expressed in the report. The findings and conclusions presented in the report are the responsibility of Sikich. The OIG's responsibility is to provide adequate oversight of the contractor's work in accordance with Generally Accepted Government Audit Standards.

Please provide planned corrective actions and expected dates to complete the actions for each of the recommendations within 30 days of the date of this report. As with all OIG products, we determine what information is publicly posted on our website from the published report. Consistent with our responsibility under the Inspector General Act of 1978, as amended, we may provide copies of our report to congressional committees oversight responsibility over NARA. We appreciate the cooperation and assistance NARA extended to us during this audit. Please contact me with any questions.

Cc:

William. J. Bosanko, Deputy Archivist of the United States
Merrily Harris, Executive Secretariat
Colleen Murphy, Acting Chief of Management and Administration
Jay Trainer, Acting Chief Operating Officer

Sheena Burrell, Chief Information Officer
Nicole Willis, Deputy Chief Information Officer
Akhtar Zaman, Chief Data Officer
Kimberly Boykin, Chief of Staff, Information Services
Damon Nevils, Acting Chief Acquisition Officer
Kimm Richards, Accountability
William Brown, Senior Program Auditor
Teresa Rogers, Senior Program Auditor
United States Senate Homeland Security and Governmental Affairs Committee
United States House of Representatives Committee on Oversight and Reform



**CLOUD COMPUTING SERVICES
PERFORMANCE AUDIT**

**SUBMITTED TO THE
NATIONAL ARCHIVES AND RECORDS ADMINISTRATION
OFFICE OF INSPECTOR GENERAL**

**PERFORMANCE AUDIT OF NARA'S
CLOUD COMPUTING SERVICES**

SEPTEMBER 27, 2024

TABLE OF CONTENTS

EXECUTIVE SUMMARY	1
SUMMARY OF RECOMMENDATIONS.....	2
BACKGROUND.....	2
AUDIT RESULTS	3
FINDING 1: NARA'S ENTERPRISE DATA INVENTORY IS INCOMPLETE.....	3
FINDING 2: NARA'S MONITORING OF SERVICE LEVEL AGREEMENTS FOR CLOUD-BASED SYSTEMS CAN BE IMPROVED.....	4
APPENDIX A: OBJECTIVE, SCOPE, AND METHODOLOGY	6
APPENDIX B: PRIOR AUDIT RECOMMENDATIONS	9
APPENDIX C: MANAGEMENT RESPONSE	11
APPENDIX D: ACRONYMS	12
APPENDIX E: REPORT DISTRIBUTION LIST.....	13
APPENDIX F: OIG HOTLINE CONTACT INFORMATION	14



333 John Carlyle Street, Suite 500
Alexandria, VA 22314
703.836.6701

SIKICH.COM

September 27, 2024

Dr. Brett Baker
Inspector General
Office of Inspector General
National Archives and Records Administration

Subject: Performance Audit of NARA's Cloud Computing Services

Dear Dr. Baker:

Sikich CPA LLC (Sikich)¹ is pleased to submit the attached report detailing the results of our performance audit of the National Archives and Records Administration's (NARA's) Cloud Computing Services conducted under contract number 88310323A00012, order number 88310323F00282. The objective of this audit was to assess NARA's efforts relating to cloud computing management. Specifically, the audit examined whether NARA has effectively implemented plans and procedures to meet federal requirements.

We conducted the audit fieldwork in Alexandria, VA, from October 2023 through August 2024. We conducted this performance audit in accordance with *Generally Accepted Government Auditing Standards*, as issued by the Comptroller General of the United States (2018 Revision, Technical Update April 2021). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We describe our objective, scope, and methodology further in **Appendix A: Objective, Scope, and Methodology**.

We would like to thank all the NARA personnel we met with or who provided artifacts for their cooperation and assistance.

Sincerely,

Sikich CPA LLC

September 27, 2024

¹ Effective December 14, 2023, we amended our legal name from "Cotton & Company Assurance and Advisory, LLC" to "Sikich CPA LLC" (herein referred to as "Sikich"). Effective January 1, 2024, we acquired CliftonLarsonAllen's (CLA's) federal practice, including its work for the National Archives and Records Administration Office of Inspector General.

EXECUTIVE SUMMARY

The National Archives and Records Administration (NARA) Office of Inspector General (OIG) engaged Sikich CPA LLC (Sikich)² to conduct a performance audit to assess NARA's efforts relating to cloud computing management.

PERFORMANCE AUDIT OF NARA'S CLOUD COMPUTING SERVICES

Why Did We Conduct this Audit?

In 2011, the Office of Management and Budget (OMB) issued the *Federal Cloud Computing Strategy* which required agencies to use cloud infrastructure, as they planned new missions, supported applications, or consolidated existing applications. In 2019, the *Federal Cloud Computing Strategy* was updated, tasking federal agencies to accelerate migration to cloud-based computing solutions and modernize information technology (IT) infrastructure. NARA, like other Federal agencies, is increasing its use and accelerating its adoption of cloud computing services.

The audit's objective was to assess NARA's efforts relating to cloud computing management. Specifically, to determine if NARA has effectively implemented plans and procedures to meet federal requirements.

To address this objective, we reviewed relevant policies, procedures, guidance, and other internal control documentation related to NARA's cloud computing strategy and its implementation of selected security controls. We also evaluated selected controls over a sample of NARA's cloud-based systems.

What Did We Recommend?

This report makes four recommendations that are intended to strengthen NARA's management of its cloud computing environment.

What Did We Find?

Overall, we found that NARA generally has effective governance processes in place to manage its cloud computing services. However, NARA has opportunities to improve management of its cloud computing management program. First, we found that NARA is still in the process of completing its enterprise data inventory. Without a complete inventory of data used in NARA's systems, there is a potential for data to be insufficiently secured. In addition, visibility into all existing cloud data helps to promote efficiency and effectiveness of NARA's operations, by identifying duplicate data collections which can be consolidated. Further, NARA may be maintaining data sets which are no longer needed and can be disposed.

Second, we found that NARA can improve its monitoring activities of service level agreements for its cloud computing services. Without centralized monitoring procedures for service level agreements, NARA is not able to consistently determine if a contractor is providing the level of service agreed upon in the contract. Furthermore, NARA may not be consistently monitoring performance measures, responding to missed metrics, and enforcing penalties, all of which could lead to inefficient use of resources and disruption to NARA's operations.

² Effective December 14, 2023, we amended our legal name from "Cotton & Company Assurance and Advisory, LLC" to "Sikich CPA LLC" (herein referred to as "Sikich"). Effective January 1, 2024, we acquired CliftonLarsonAllen's (CLA's) federal practice, including its work for the NARA OIG.

SUMMARY OF RECOMMENDATIONS

Number	Recommendation	Responsible Office
1.	Complete the enterprise-wide data inventory.	Chief Information Officer
2.	Document and implement a standard operating procedure to maintain the enterprise-wide data inventory as new data collections are created and old data collections are retired.	Chief Information Officer
3.	Collaborate with NARA's Chief Information Officer to document and implement a standardized process to monitor service level agreements with cloud-based service providers. The process should include the monitoring responsibilities of the Contracting Officer's Representatives and actions NARA should take if a contractor does not meet the defined service levels.	Chief Acquisition Officer and Chief Information Officer
4.	Document and implement a process to incorporate the Cloud Service Provider's Quality Assurance Surveillance Plan as part of future cloud service contracts. Where incorporation of a Cloud Service Provider Quality Assurance Surveillance Plan is not anticipated, NARA should incorporate its own Quality Assurance Surveillance Plan and service level agreements at the solicitation phase, these should align with commercial best practices.	Chief Acquisition Officer

BACKGROUND

NARA is an independent agency within the executive branch of the federal government responsible for preserving, protecting, and providing access to the records of our government. NARA is directed by the Archivist of the United States who is appointed by the President of the United States, with the advice and consent of the Senate. NARA's operations rely on 20 cloud computing systems providing an array of services. Total Information Technology (IT) spending by NARA represents an annual investment of approximately \$156.8 million.³

In 2011, the Office of Management and Budget (OMB) issued its *Federal Cloud Computing Strategy* which required agencies to use cloud infrastructure, as they planned new missions, supported applications, or consolidated existing applications. In 2019, the *Federal Cloud Computing Strategy* was updated, tasking federal agencies to accelerate migration to cloud-based computing solutions and modernize IT infrastructure. The strategy focused on enhancing security and high-quality IT service to the American people. In May 2021, the President issued an Executive Order⁴ detailing his administration's goal to modernize federal government cybersecurity. Specifically, to keep pace with today's dynamic and increasingly sophisticated environment, the federal government should accelerate the movement to secure cloud services, adopt security best practices, and develop migration plans for Zero Trust Architecture.⁵

³ IT Portfolio Dashboard for NARA <https://www.itdashboard.gov/itportfoliodashboard>.

⁴ Executive Order 14028, *Improving the Nation's Cybersecurity* (May 12, 2021) <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>

⁵ Executive Order 14028 defines the term "Zero Trust Architecture" as a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. The Zero Trust security model eliminates implicit

NARA, like other Federal agencies, is increasing its use and accelerating its adoption of cloud computing services. The National Institute of Standards and Technology (NIST) defines cloud computing as a model for enabling 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.⁶

NARA has created an *Enterprise Multi-Cloud Strategy* to document their approach of implementing cloud computing services, including the establishment of a Cloud Center of Excellence. The Cloud Center of Excellence serves as NARA's centralized control tower providing executive oversight of NARA's current and future cloud systems. The Cloud Center of Excellence also creates NARA's cloud policies as well as provides guidance to internal NARA personnel on different cloud architectures and cloud solutions. The *Enterprise Multi-Cloud Strategy* also defines roles and responsibilities related to cloud computing services. For example, Systems Engineering Division (part of the Chief Technology Officer's organization) is responsible for the overall design and capacity planning of cloud systems. Finally, the Office of the Chief Acquisition Officer is responsible for overseeing cloud-based acquisition agreements.

AUDIT RESULTS

NARA could improve management of its cloud computing program by maintaining a complete enterprise data inventory and implementing a process to monitor service level agreements with cloud-based service providers. Below, we provide detailed information regarding each finding.

Finding 1: NARA's Enterprise Data Inventory is Incomplete

OMB Circular A-130, *Managing Information as a Strategic Resource* (July 2016), establishes the requirements for agencies to develop an enterprise-wide data inventory. The Open, Public, Electronic, and Necessary Government Data Act (OPEN Data Act) provides clarifying information regarding enterprise-wide data inventories. Specifically, the OPEN Data Act states that an enterprise data inventory accounts for any data asset created, collected, under the control or direction of, or maintained by the agency.⁷ Creating and maintaining an enterprise data inventory allows an agency to develop a clear and comprehensive understanding of the data assets in its possession. With this comprehensive understanding, the agency can better develop safeguards and protections for its data.

While NARA has completed an inventory of data that is available to the public, it has not completed an enterprise-wide data inventory that includes non-public data maintained in NARA systems.

NARA initiated a draft of the Data Inventory several years ago, but NARA management indicated the delay in finalizing this inventory has been in part due to the lack of resources and conflicting priorities.

trust in any one element, node, or service and instead requires continuous verification of the operational picture via real-time information from multiple sources to determine access and other system responses.

⁶ NIST Special Publication 800-145, *The NIST Definition of Cloud Computing* (September 2011).

⁷ Public Law (Pub. L.) No. 115-435, 132 Stat. 5529 (2019). Requirements for Federal agencies to improve Federal data management are codified at 44 U.S. Code (U.S.C.), available at <https://www.congress.gov/bill/115th-congress/house-bill/1770/text>

OMB Circular A-130, *Managing Information as a Strategic Resource* (July 2016), Section 5.a.1.a, states:

Agencies shall:

- i. Maintain an inventory⁸ of the agency's major information systems,⁹ 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;*

Without a complete inventory of data used in NARA's systems, there is a potential for data to be insufficiently secured. In addition, visibility into all existing cloud data helps to promote efficiency and effectiveness of NARA operations, by identifying duplicate data collections which can be consolidated. Further, NARA may be maintaining data sets which are no longer needed and can be disposed.

We recommend that the NARA Chief Information Officer:

Recommendation 1: Complete the enterprise-wide data inventory.

Recommendation 2: Document and implement a standard operating procedure to maintain the enterprise-wide data inventory as new data collections are created and old data collections are retired.

Finding 2: NARA's Monitoring of Service Level Agreements for Cloud-Based Systems Can Be Improved

NARA could not provide evidence demonstrating service level agreements were being monitored for four out of four sampled cloud system's contracts.

NARA did not have a documented process in place for Contracting Officer's Representatives to document their monitoring activities of service level agreements in cloud computing contracts. In addition, NARA does not have a process in place to review contracts for cloud systems to ensure service level agreements are consistently documented and used to facilitate contract management oversight.

OMB's *Federal Cloud Computing Strategy* (June 2019), states the following:

A service level agreement between a customer and a service provider defines the level of performance expected from a service provider, how that performance will be measured, and what enforcement mechanisms will be used to ensure the specified levels are achieved.

...

Therefore, to facilitate effective risk management by way of their relationships with commercial cloud service providers, agencies should granularly articulate roles and

⁸ The inventory of agency information resources shall include an enterprise-wide data inventory that accounts for data used in the agency's information systems.

⁹ The inventory of major information systems is required in accordance with 44 U.S.C. § 3505(c). All information systems are subject to the requirements of the Federal Information Security Modernization Act (44 U.S.C. Chapter 35), whether or not they are designated as a major information system.

responsibilities, establish clear performance metrics, and implement remediation plans for non-compliance.

In addition, the Chief Information Officer's (CIO's) Council and Chief Acquisition Officers Council, *Creating Effective Cloud Computing Contracts for the Federal Government, Best Practices for Acquiring IT as a Service* (February 2012) states the following:

Federal agencies should ensure that [Cloud Service Provider] (CSP) performance is clearly specified in all [service level agreements] (SLAs), and that all such agreements are fully incorporated, either by full text or by reference, into the CSP contract.

Furthermore, Federal Acquisition Regulation (FAR) Subpart 37.5, *Management Oversight of Service Contracts*, states the following regarding contracting officials' responsibilities:

Contracting officials should ensure that "best practices" techniques are used when contracting for services and in contract management and administration.

FAR Subpart 37.5 defines best practices as techniques gained from experience that agencies may use to help detect problems in the acquisition, management, and administration of service contracts or to improve the procurement process.

Finally, the Government Accountability Office's (GAO's) *Standards for Internal Control in the Federal Government* (September 2014), states the following regarding management's responsibility for monitoring activities:

Management should establish and operate monitoring activities to monitor the internal control system and evaluate the results.

Without centralized monitoring procedures for service level agreements, NARA is not able to consistently determine if a contractor is providing the level of services agreed upon in the contract. Furthermore, NARA may not be consistently monitoring performance measures, responding to missed metrics, and enforcing penalties, all of which could lead to inefficient use of resources and disruption to NARA's operations.

We recommend that the NARA Chief Acquisition Officer:

Recommendation 3: Collaborate with NARA's Chief Information Officer to document and implement a standardized process to monitor service level agreements with cloud-based service providers. The process should include the monitoring responsibilities of the Contracting Officer's Representatives and actions NARA should take if a contractor does not meet the defined service levels.

Recommendation 4: Document and implement a process to incorporate the Cloud Service Provider's Quality Assurance Surveillance Plan as part of future cloud service contracts. Where incorporation of a Cloud Service Provider Quality Assurance Surveillance Plan is not anticipated, NARA should incorporate its own Quality Assurance Surveillance Plan and service level agreements at the solicitation phase, these should align with commercial best practices.

APPENDIX A: OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The objective of this performance audit was to assess NARA's efforts relating to cloud computing management. Specifically, we examined whether the agency has effectively implemented plans and procedures to meet federal requirements.

Scope

Our audit scope covered internal controls, processes, and procedures related to NARA's cloud computing management in place from October 2023 through August 2024. To assess NARA's efforts in this area, we evaluated the following:

- NARA's computing strategy and cloud architecture approach.
- NARA's cloud data governance processes.
- Roles and responsibilities for cloud systems.
- NARA's cloud computing system inventory.
- Key selected controls from NIST Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, for a sample of NARA's cloud system implementations.

Methodology

We conducted this performance audit in accordance with *Generally Accepted Government Auditing Standards* (2018 Revision, Technical Update April 2021). Those standards require that we plan and perform the audit to obtain sufficient appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We conducted the audit fieldwork in Alexandria, Virginia from October 2023 through August 2024.

To accomplish our audit objectives, we completed the following procedures:

- Inquired of NARA personnel responsible for the procurement, development, and maintenance of NARA's cloud-based systems.
- Inspected applicable Federal regulations, standards and best practices, as well as NARA policies and procedures related to cloud computing, including but not limited to:
 - OMB *Federal Cloud Computing Strategy* (June 2019).
 - OMB Circular A-130, *Managing Information as a Strategic Resource* (July 2016).
 - NIST Special Publication 800-145, *The NIST Definition of Cloud Computing* (September 2011).
 - NARA, *Enterprise Multi-Cloud Strategy* (August 2021).
 - NARA, *Migrating a System into the Enterprise Cloud Environment Standard Operating Procedure* (April 2020).
 - NARA, *Cloud Provisioning Guidelines*.

- NARA, *Enterprise Multi-Cloud Services Cloud Center of Excellence Charter* (May 2022).
- CIO's Council and Chief Acquisition Officers Council, *Creating Effective Cloud Computing Contracts for the Federal Government, Best Practices for Acquiring IT as a Service* (February 2012).
- Evaluated select security processes and controls for a non-statistical sample of 4 NARA cloud-based systems from the 20 systems in NARA's system inventory extract. In order to select the sample of systems, we inspected the NARA population of cloud systems and selected systems that were hosted with different cloud service providers. This sample design was selected to ensure different cloud service providers were selected to determine if NARA was implementing security controls equally across all cloud service providers. Since this sample is non-statistical, the results from our testing cannot be projected to the population.
- Analyzed the sample of four systems selected for testing, including reviewing selected system documentation such as system security plans, risk assessments, contracts, and service level agreements.
- Inspected the NARA Enterprise Data Inventory to determine if all data collections were properly documented and accounted for.
- Reviewed the status of open audit recommendations from the *Audit of NARA's Adoption and Management of Cloud Computing* (Audit Report Number 17-AUD-08, March 15, 2017).¹⁰ See **Appendix B** for the status of the open recommendations.

We assessed internal controls that we deemed to be significant to the audit objective. Specifically, we assessed 6 of the 17 principles associated with the 5 components of internal control defined in the GAO's *Standards for Internal Controls in the Federal Government* (September 2014) (the Green Book). The table below summarizes the principles we assessed:

Table 1: GAO Green Book Assessment Principles

Control Environment
Principle 3: Management should establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives.
Risk Assessment
Principle 7: Management should consider the potential for fraud when identifying, analyzing, and responding to risks.
Control Activities
Principle 10: Management should design control activities to achieve objectives and respond to risks.
Principle 11: Management should design the entity's information system and related control activities to achieve objectives and respond to risks.
Monitoring
Principle 16: Management should establish and operate monitoring activities to monitor the internal control system and evaluate the results.
Principle 17: Management should remediate identified internal control deficiencies on a timely basis.

We assessed the design, implementation, and/or operating effectiveness of these internal controls and identified deficiencies that we believe could affect NARA's ability to effectively manage its cloud computing services. The internal control deficiencies we found are discussed

¹⁰ <https://www.oversight.gov/sites/default/files/oig-reports/audit-report-17-08.pdf>



in the Audit Results section of this report. However, because our review was limited to aspects of these internal control components and underlying principles, it may not have disclosed all internal control deficiencies that may have existed at the time of this audit.

APPENDIX B: PRIOR AUDIT RECOMMENDATIONS

Below is the status of recommendations from the NARA OIG *Audit of NARA's Adoption and Management of Cloud Computing* (Audit Report Number 17-AUD-08, March 15, 2017)¹¹, that were open as of October 3, 2023. Recommendation 5 was previously closed and therefore is not reported here.

Recommendation Number	Recommendation	Status
1	The NARA CIO, acting as 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.	Closed.
2	The NARA CIO should complete and document a review of existing IT systems for cloud compatibility.	Closed.
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.	Closed.
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.	Open.
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.	Open.
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.	Closed.
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.	Closed.

¹¹ <https://www.oversight.gov/sites/default/files/oig-reports/audit-report-17-08.pdf>

Recommendation Number	Recommendation	Status
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.	Subsumed into the new recommendation 3 of this report.
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 [Capital Planning and Investment Control] (CPIC) Business Case Form.	Open.

APPENDIX C: MANAGEMENT RESPONSE

Agency management stated their general agreement with the findings and recommendations and opted not to provide formal comments for inclusion in this report.

APPENDIX D: ACRONYMS

Acronym	Definition
CIO	Chief Information Officer
CPIC	Capital Planning and Investment Control
CSP	Cloud Service Provider
FAR	Federal Acquisition Regulation
GAO	Government Accountability Office
IT	Information Technology
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPEN Data Act	Open, Public, Electronic, and Necessary Government Data Act
U.S.C.	United States Code

APPENDIX E: REPORT DISTRIBUTION LIST

Archivist of the United States

Deputy Archivist of the United States

Executive Secretariat

Acting Chief of Management and Administration

Acting Chief Operating Officer

Chief Information Officer

Deputy Chief Information Officer

Chief Data Officer

Chief of Staff, Information Services

Acting Chief Acquisition Officer

Accountability

United States Homeland Security and Governmental Affairs Committee

United States House of Representatives Committee on Oversight and Reform

APPENDIX F: OIG HOTLINE CONTACT INFORMATION

The OIG Hotline provides a confidential channel for reporting fraud, waste, abuse, and mismanagement to the OIG. In addition to receiving telephone calls at a toll-free Hotline number, we also accept emails through an online referral form. Walk-ins are always welcome. Visit <https://naraoig.oversight.gov/> for more information, or contact us:

Contact the OIG Hotline [Online Complaint Form](#)

Contact the OIG by telephone and FAX

Hotline Telephone: 301-837-3500 (local) or 1-800-786-2551 (toll-free)
FAX: 301-837-3197

Contractor Self-Reporting Hotline

As required by the Federal Acquisition Regulation, a web-based form allows NARA contractors to notify the OIG, in writing, whenever the contractor has credible evidence a principal, employee, agent, or subcontractor of the contractor has committed a violation of the civil False Claims Act or a violation of Federal criminal law involving fraud, conflict of interest, bribery, or gratuity violations in connection with the award, performance, or closeout of a contract or any related subcontract. The form can be accessed through the OIG's home page or found directly at [Contractor Reporting Form](#).