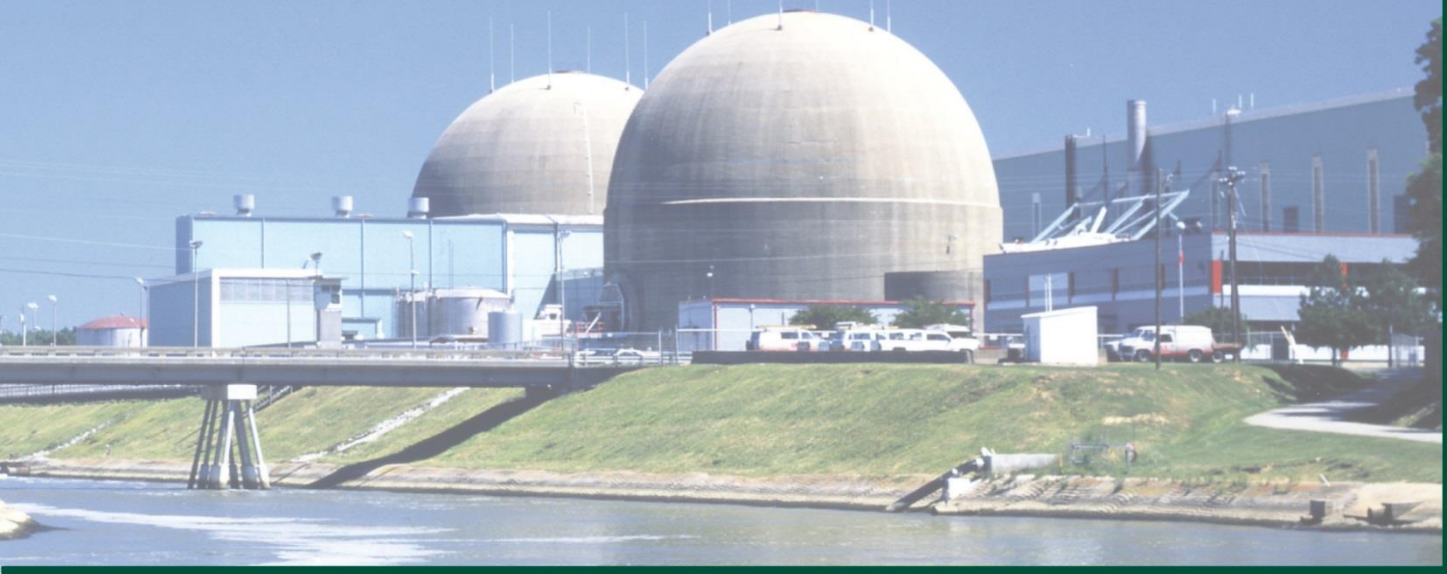
OFFICE OF THE INSPECTOR GENERAL

U.S. NUCLEAR REGULATORY COMMISSION
DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Audit of NRC's Adoption of Cloud Computing

OIG-17-A-16
June 20, 2017



All publicly available OIG reports (including this report) are accessible through NRC's Web site at
http://www.nrc.gov/reading-rm/doc-collections/insp-gen

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

OFFICE OF THE
INSPECTOR GENERAL

June 20, 2017

MEMORANDUM TO: Victor M. McCree
Executive Director for Operations

FROM: Dr. Brett M. Baker ***/RA/***
Assistant Inspector General for Audits

SUBJECT: AUDIT OF NRC'S ADOPTION OF CLOUD COMPUTING (OIG-17-A-16)

Attached is the Office of the Inspector General's (OIG) audit report titled *Audit of NRC's Adoption of Cloud Computing*.

The report presents the results of the subject audit. Following the June 8, 2017, exit conference, agency staff indicated that they had no formal comments for inclusion in this report.

Please provide information on actions taken or planned on each of the recommendations within 30 days of the date of this memorandum. Actions taken or planned are subject to OIG followup as stated in Management Directive 6.1.

We appreciate the cooperation extended to us by members of your staff during the audit. If you have any questions or comments about our report, please contact me at (301) 415-5915 or Beth Serepca, Team Leader, at (301) 415-5911.

Attachment: As stated

Office of the Inspector General

U.S. Nuclear Regulatory Commission
Defense Nuclear Facilities Safety Board

OIG-17-A-16

June 20, 2017

Results in Brief

Why We Did This Review

Adoption of cloud computing became Federal policy in 2010. The policy prodded agencies to consolidate data centers, consider cloud services first in new acquisitions, use shared services, and adapt activities to new information technology (IT) service models.

Cloud computing is defined as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources.

A significant IT services contracting effort is underway at the Nuclear Regulatory Commission (NRC). Several cloud applications have been recently deployed. The agency also is obtaining technical support for future cloud planning, acquisitions, and deployment.

The audit objective was to assess whether NRC's adoption of cloud computing is adequately managed.

Audit of NRC's Adoption of Cloud Computing

What We Found

NRC has not had a cohesive approach to cloud adoption. Federal and NRC guidance emphasize management's role in providing objectives, resources, and oversight for IT projects. However, until 2016, NRC management's focus on the agency's data centers substituted for an effective cloud strategy.

For example, NRC management committed to consolidating two older data centers into its new Three White Flint North data center. The decision was made without completing a cloud alternatives study that would have not only defined a basis for determining which options best met NRC's requirements, but also provided complete cost analysis of cloud and internal options.

The consolidation resulted in resources that are not scalable, rapidly provisioned, or shared. Further, it did not realize expected operating cost savings. Due to a lack of cost analysis in the beginning, it is not clear whether the project's modernization benefits were worth the additional cost, or whether the same benefits could have been achieved at a lower cost while also enabling the adoption of effective cloud solutions.

What We Recommend

The report makes two recommendations to develop guidelines to ensure that cloud services acquisitions rely on thorough project planning, and to train NRC information technology and acquisitions staff to manage new models of service delivery. Management stated their agreement with the findings and recommendations in this report.

TABLE OF CONTENTS

ABBREVIATIONS AND ACRONYMS

3WFN	Three White Flint North
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Modernization Act
GLINDA	Global Infrastructure and Development Acquisition
IaaS	Infrastructure as a Service
IM	Information Management
IT	Information Technology
IT/IM	Information Technology/Information Management
ITISS	Information Technology Infrastructure and Support Services
MD	Management Directive
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
OCIO	Office of the Chief Information Officer
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OWFN	One White Flint North
PaaS	Platform as a Service
SaaS	Software as a Service
TTC	Technical Training Center
TWFN	Two White Flint North

I. BACKGROUND

Adoption of cloud computing became Federal policy with the Office of Management and Budget's (OMB) issuance of the "25-Point Implementation Plan for Reform of Federal Information Technology Management" (25-Point Plan) in December, 2010. Several of the 25 points provided impetus for the Nuclear Regulatory Commission (NRC) to consider changes that would promote adoption of cloud services, including consolidate Federal data centers; consider "cloud first" in new information technology (IT) projects; use shared services; and develop IT program management and IT acquisitions professionals.

The National Institute of Standards and Technology (NIST) defined five key cloud characteristics[1] (see sidebar). In summary, a customer can use the cloud service it needs, when it needs it, and be billed according to use.

NIST also described service models, with different capabilities:

- Infrastructure as a Service (IaaS) – to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy software, including operating systems and applications; the consumer retains control over operating systems, storage, and deployed applications, and may select networking components.

NIST Cloud Characteristics

- Measured service: Easily measured usage for metering costs.
- On demand: Changes to the service usage levels must be easy, timely, no management involvement.
- Broad access: Must be accessible from any computer with internet access.
- Resource pooling: Computing power and storage resources are pooled and can be shared by separate customers.
- Elasticity: Elastic and can be scaled up or scaled down depending on how much usage a customer wants to purchase.

Source: NIST SP-800-145

[1] NIST Special Publication 800-145, *Definition of Cloud Computing* (2011)

- Platform as a Service (PaaS) – to deploy onto the cloud infrastructure consumer-created or acquired applications, but the consumer does not manage or control the underlying cloud infrastructure, only the deployed applications.
- Software as a Service (SaaS) – to use the provider's applications running on a cloud infrastructure; the consumer does not control cloud infrastructure or most application capabilities.

The three service models offer progressively less customer control, but also entail progressively fewer consumer requirements and resources for IT management.

Current Status

Responsible Offices

NRC's Office of the Chief Information Officer (OCIO) is responsible for adopting cloud computing, as part of its overall responsibilities for planning, directing, and overseeing the delivery of centralized IT infrastructure, applications, and information management (IM) services, and the development and implementation of plans, architecture, and policies to support the mission, goals, and priorities of the agency. OCIO is supported by the Acquisition Management Division of the Office of Administration, which provides advice and assistance relative to meeting program and mission objectives consistent with procurement requirements.

Global Infrastructure and Development Acquisition

In 2011, NRC awarded the Information Technology Infrastructure and Support Services (ITISS) contract for up to 6 years as a single award contract to Dell Services Federal Government. The ITISS contract provides agency-wide IT and IM infrastructure and support services under a single, primary provider and broker for various areas of IT services. The ITISS contract with Dell's successor, NTT Data Services Federal Government, will soon expire. OCIO has worked with acquisitions specialists to develop a new multi-award contract, Global Infrastructure and Development Acquisition (GLINDA). GLINDA divides the services provided under ITISS into four separate areas. Services provided must be approved under the Federal Risk and Authorization Management Program

(FedRAMP).[2] GLINDA's multiple awardees will compete for task orders in each area to offer NRC the best value.

Cloud Developments

NRC is actively implementing cloud solutions. Systems that were already externally hosted have seen their hosts move to the cloud, and the agency is adopting SaaS solutions. Standalone systems that periodically require a high volume of computing power will migrate to IaaS. Within GLINDA, NRC is seeking broker-like services[3] to provide cloud service planning and design advisory and technical expertise. Appendix B presents detail on the agency's cloud strategy and service developments during the course of this audit.

II. OBJECTIVE

The audit objective was to assess whether NRC's adoption of cloud computing is adequately managed.

III. FINDING

While NRC has been slow to adopt cloud services, the agency's current strategy and activities demonstrate an informed, deliberate course for cloud adoption with strong management support. However, NRC management must take steps to ensure that the effort and understanding reflected in the current strategy are not lost in the face of continuing operating challenges.

[2] FedRAMP is a Government wide program that promotes a cost-effective, risk-based approach to cloud services adoption by providing Federal agencies with a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

[3] A cloud broker-like service will provide technical expertise as an intermediary between NRC, as cloud service purchaser, and cloud service providers, but will not negotiate contracts on behalf of the agency.

NRC Has Not Had a Cohesive Approach to Adopting Cloud Services

Management is responsible for providing the objectives, organizational structure, and resources for the development and management of IT projects. NRC's focus on data centers substituted for an effective cloud strategy because management's short-term vision and conservatism hampered cloud adoption. The resulting delay in adoption of cloud services impeded optimal use of resources.

What Is Required

Management Must Provide Support for Effective IT Program Management

Management is responsible for providing the objectives, organizational structure, and resources to support successful IT program management. Management can anticipate and plan for significant changes in the entity's environment by using a forward-looking planning process.

Federal Guidance

Agency management must implement a process to maximize the value of the agency's IT investments and assess, manage, and evaluate the risks. Successful Federal IT projects need the support of senior management through securing funding, ensuring consistent, knowledgeable staffing, helping to resolve challenges, and reaching out to stakeholders. Defining objectives and detailed work breakdown are keys to estimating, budgeting, planning, and monitoring costs and schedules. With well-prepared estimates and plans, management can resolve problems and promote accountability at all levels and stages of a project. These factors are also consistent with industry practices for IT acquisitions and best practices relating to risk management and governance.

NRC Guidance

NRC's Management Directive (MD) 2.8, *Integrated Information Technology/Information Management (IT/IM) Governance Framework*

(2016), states that the governance function ensures that programs align with the agency's strategic goals, priorities, and technology standards. Senior management is assigned oversight and key roles in planning, budget formulation, and monitoring IT projects. Management must define agency IT/IM plans, technical standards, and other guidance.

As OMB's 25-Point Plan directed a cultural shift from custom systems to shared services, it also affirmed the role of agency management in supporting the change. MD 2.8 notes project management for cloud-based service involves provisioning and deployment, and these new approaches dictate a fundamental shift in IT/IM project management at NRC.

What We Found

Focus on Data Centers Substituted for an Effective Cloud Strategy

Until 2016, NRC management's focus emphasized modifications to the agency's data centers.

While NRC installed a new data center in the new Three White Flint North building (3WFN) to support office moves during 2013, the agency also considered how it could adopt cloud services and how to manage its other data centers in conflicting ways.

- A 2013 cloud strategy document discussed foundational, developmental, and cloud service delivery initiatives in a multi-phase, long term effort. Ongoing data services would continue in 3WFN, while NRC took the preparatory step of building a scalable, self-provisioning internal "private cloud" environment to give technical and financial experience for adopting public cloud services.

- At the same time in 2013, the agency requested a proposal for data center migration from the incumbent contractor under ITISS. Although it referred to the cloud strategy document, the task request envisioned partial reuse of existing equipment to lower costs. The project would begin with the One White Flint North (OWFN) and Two White Flint North (TWFN) data centers, with a

schedule for migration of the regional and Technical Training Center (TTC) data centers within 2 fiscal years.

Although management asserted that over the longer term NRC would reduce reliance on internal data centers, NRC committed to migration of the OWFN and TWFN data centers to the new 3WFN facility. The contractor referred to the consolidation and virtualization project as a "private cloud" although its resources would not be scalable, rapidly provisioned, or shared.

Migration and closing of OWFN and TWFN data centers were completed in fiscal years 2015 and 2016, respectively, at a cost of $3.6 million with replacement of the existing equipment. Operating expenses were then based on firm fixed price leasing of the new equipment and the setup of virtualized machines. Although NRC had originally planned the migration of regional and TTC data centers to follow consolidation of the headquarters data centers, these actions were deferred. The project's net reduction of data centers was therefore one.

An updated cloud strategy developed for NRC at the end of 2015 noted that the "general efficacy and value of public cloud alternatives for efficient delivery of infrastructure services is undisputed," yet the strategy still focused on maintaining the 3WFN data center and its systems with little change. Its proposed connection of the existing data center to a public cloud service would enable incremental change, but it still deferred identifying appropriate solutions for specific NRC systems and applications.

Why This Occurred

Short-Term Vision and Conservatism Hampered Cloud Adoption

Faced with multiple Federal mandates and budget uncertainties, NRC management made decisions regarding cloud adoption based on meeting short term goals without multiyear planning and budgeting. Data center changes appeared to offer a single solution for multiple demands, while

planning and decision making for cloud services were consistently deferred.

Incomplete Data Center Study

NRC completed one part of a three-part "data center alternatives" study in June, 2012. Part one of the study evaluated co-location of the OWFN and TWFN data centers in onsite and various external hosting environments, but assumed the agency would continue to need and fully support the 3WFN data center. Given this assumption, this study phase concluded that considering co-location alone appeared to favor an onsite option, but stated external options should not be ruled out without completing the analysis. However, management ended the data center alternatives study after the review of co-location, and decided to focus resources on the 3WFN facility.

This decision omitted necessary information from the other two parts of the alternatives study that would have provided a full understanding of business opportunities and costs of different options. The decision asserted that in the long term, NRC would look for ways to reduce reliance on internal data centers.

Unaddressed Staff Concerns

Further, decisions did not always address concerns of knowledgeable staff. A staff team that evaluated the 2013 data center migration proposal determined it jeopardized NRC's ability to compare the proposed solution to potentially innovative and cost effective solutions from other vendors. The assessment team concluded that the proposal placed NRC in the position of adapting its cloud strategy to an existing service provider because it lacked the following:

- A cost analysis that compared the current costs of the services used to the costs of the proposed solution for similar services.
- A defined exit strategy, risking vendor "lock-in" where the NRC could lose control over the direction, timing, implementation, and future expansion of its cloud strategy and cloud migration.
- A basis to decide if the services proposed meet the NRC's availability, service delivery, and other requirements.

Management opted to use the incumbent contractor for migration of existing data centers to the 3WFN environment despite staff concerns.

Conservative Security

The key reason given for the decision to consolidate the data centers instead of pursuing a cloud solution was that the NRC Information Technology Infrastructure System and Data Center Services were authorized at the Federal Information Security Modernization Act (FISMA) 'High' impact level. However, according to NRC staff, many systems that were rated 'High' (severe or catastrophic adverse effect) could have been rated 'Moderate' (serious adverse effect), which would have supported adoption of cloud solutions.

Why This Is Important

Delay of Cloud Services Adoption Impeded Better Resource Use

Management's continued focus on consolidating and updating the 3WFN data center delayed adoption of cloud solutions by NRC.

Data center migration to 3WFN provided modernized equipment and increased virtualization in a new facility, but at a cost. One estimate of the cost of operating the aging OWFN and TWFN data centers was $6.5 million per year. In 2012, the transition cost of moving 145 racks from OWFN and TWFN was estimated at $3.6 million, and operating expenses for the co-located data centers in 3WFN were estimated at an average of $4 million per year. However, after the $3.6 million migration and modernization, operating the consolidated 3WFN data center cost up to $7.5 million per year. As shown in Table 1, expected cost savings were not realized.

Table 1: Comparison of Data Center Costs

Facility	Move	Monthly Operation (average)	Annual operation	5-year total
OWFN/TWFN (estimated)	N/A	$541 thousand	$6.5 million	$32.5 million
Co-locate OWFN/TWFN in 3WFN (estimated)	$3.6 million	$333 thousand	$4.0 million	$20 million
Migrate and upgrade/virtualize into 3WFN (actual)	$3.6 million	$623 thousand	$7.5 million	$37.4 million

Source: NRC documents

Further, because NRC maintained the FISMA 'High' risk impact levels for many of its IT systems, NRC may have missed opportunities to reduce lifecycle costs for some of these systems.

Adhering to a "single provider" approach within NRC's ITISS contract precluded taking advantage of competition for better value while adopting appropriate cloud or shared services.

Due to a lack of clear cost analysis from the beginning, it is impossible to determine whether the modernization benefits were worth the additional cost, or even whether the same benefits could have been achieved at a lower cost while also enabling the adoption of effective cloud solutions.

Recommendations

OIG recommends that the Executive Director for Operations

1. Develop guidelines for new IT cloud service contracts to include the following:

    a. Use of thorough project planning to include cost estimates and budgeting.
    b. Monitoring cost to sustain delivery of services.
    c. Access to active and archived data.
    d. Exit strategies.

2. Train NRC contracting and IT staff for new models of IT services.

IV. AGENCY COMMENTS

An exit conference was held with the agency on June 8, 2017. Prior to this meeting, after reviewing a discussion draft, agency management stated they had no comments on this report. As a result, agency management stated their general agreement with the finding and recommendations in this report and opted not to provide formal comments for inclusion in this report.

Appendix A

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The audit objective was to assess whether NRC's adoption of cloud computing is adequately managed.

Scope

The audit focused on NRC's adoption of cloud computing. OIG conducted this performance audit from January 2017 to May 2017 at NRC headquarters (Rockville, MD). Internal controls related to the audit objectives were reviewed and analyzed. Throughout the audit, auditors considered the possibility of fraud, waste, and abuse in the program.

Methodology

To accomplish the audit objective, OIG reviewed relevant Federal requirements, guidance, and policies. OIG analyzed NRC IT planning, strategic, budget, and procurement documents to determine the past and current adoption strategy.

Documents reviewed include

- National Institute of Standards and Technology (NIST) Special Publications, including
  - SP 800-144, *Guidelines on Security and Privacy in Public Cloud Computing* (2011).
  - SP 800-145, *Definition of Cloud Computing* (2011).
  - SP 800-146, *Cloud Computing Synopsis and Recommendations* (2012).
- Federal Risk and Authorization Management Program (FedRAMP), *Security Assessment Framework* (2015).
- Office of Management and Budget, *25 Point Implementation Plan to Reform Federal Information Technology Management* (2010).

- Office of Management and Budget, *Federal Cloud Computing Strategy* (2011).
- Office of Management and Budget, Circular No. A-130, *Management of Federal Information Resources* (2000).
- Public Law 107–347, *E-Government Act of 2002*, Title II, Federal Management and Promotion of Electronic Government Services, and Title III, Information Security.
- U.S. Government Accountability Office, *Cost Estimating and Assessment Guide* (2009).
- U.S. Government Accountability Office, *Standards for Internal Control in the Federal Government* (2014).
- U.S. Government Accountability Office, *Schedule Assessment Guide* (2015).
- U.S. Government Accountability Office, *Critical Factors Underlying Successful Major Acquisitions* (2011).
- NRC Management Directives (MD), including
    - MD 2.6, *Information Technology Infrastructure* (2005).
    - MD 2.8, *Integrated Information Technology/Information Management (IT/IM) Governance Framework* (2016).
    - MD 11.1, *NRC Acquisition of Supplies and Services* (2014).
    - MD 12.5, *NRC Cybersecurity Program* (2015).
- NRC data center and cloud computing proposals and contracting documents, and cloud strategy documents and presentations.

OIG conducted interviews of NRC staff to gain an understanding of the roles and responsibilities, internal procedures and controls, and the cloud computing adoption strategy. OIG interviewed NRC staff in OCIO, the Office of Nuclear Regulatory Research, and the Office of the Chief Financial Officer.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The audit was conducted by Beth Serepca, Team Leader; Amy Hardin, Audit Manager; Felicia Silver, Senior Auditor; Chanel Stridiron, Auditor, and Connor McCune, Auditor.

Appendix B

RECENT NRC CLOUD ACTIVITIES

NRC's current cloud adoption strategy reflects a determined shift from its prior approach. As such, notable advances in cloud adoption during the course of this audit have strengthened the overall approach and point to success of cloud computing at NRC.

NRC's current cloud computing adoption strategy has several facets.

- Engage a cloud broker-like service to provide continuous cross-cutting cloud service planning and design advisory as well as technical expertise.
- Deploy different service models as appropriate, emphasizing Software as a Service for simplest deployment, Platform as a Service to enable technology standardization, and Infrastructure as a Service minimally, for unique applications.
- Use an incremental, iterative approach that applies lessons learned and resource savings to new projects.
- Develop a service delivery model to align with the new information technology model of cloud services.
- Use FedRAMP approved services exclusively to achieve cost effective security, privacy, and other risk management capabilities.

NRC made some major steps in addition to developing its cloud strategy and contracting mechanism.

- Financial Accounting and Integrated Management Information System is an example of an externally hosted system whose host moved to the cloud in 2016. The transition was confirmed with a successful disaster recovery test.
- MaaS360 mobility service was deployed in 2015 and significantly reduced costs of government-provided mobility devices.
- NRC systems were reviewed for suitability and priority for cloud migration, including review of security categorization.
- Solutions were evaluated for providing secure, cost effective bandwidth to support cloud services.
- Staff reorganization prepared for new IT management structures.

- An appropriate contract vehicle was identified for moving High Performance Computing Systems to Infrastructure as a Service.

Pending activities include

- Aggressively completing the milestone schedule for Software as a Service products for email and collaboration tools.
- Early launch of cloud computing solutions such as Office 365. For example, deployment of Outlook in Office 365 should be completed by the end of fiscal year 2017 and alone is expected to save NRC over $1 million annually.
- Actively considering strategies for managed services for unified telecommunications.
- Incorporating extensive cost analysis for future cloud computing contracts.
- Acquiring a cloud broker service.
- Administering contractual changes to allow for competition amongst vendor awardees.

TO REPORT FRAUD, WASTE, OR ABUSE

Please Contact:

Email: Online Form

Telephone: 1-800-233-3497

TTY/TDD: 7-1-1, or 1-800-201-7165

Address: U.S. Nuclear Regulatory Commission
Office of the Inspector General
Hotline Program
Mail Stop O5-E13
11555 Rockville Pike
Rockville, MD 20852

COMMENTS AND SUGGESTIONS

If you wish to provide comments on this report, please email OIG using this link.

In addition, if you have suggestions for future OIG audits, please provide them using this link.