



U.S. Department of Energy
Office of Inspector General
Office of Audits and Inspections

AUDIT REPORT

The Department of Energy's Management of
Cloud Computing Activities

DOE/IG-0918


September 2014



Department of Energy
Washington, DC 20585

September 19, 2014

MEMORANDUM FOR THE SECRETARY

FROM: 
Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Audit Report on "The Department of Energy's Management of Cloud Computing Activities"

BACKGROUND

Cloud computing enables convenient, on-demand access to shared computing resources that can be rapidly provided to users. The Office of Management and Budget (OMB) established the *Federal Cloud Computing Strategy* because of the significant potential to reduce the cost of Federal information technology systems, while improving capabilities and stimulating innovation in information technology solutions. As part of this strategy, OMB instituted a "Cloud First" policy designed to accelerate the pace with which cloud computing technologies are adopted and used by the Federal government. In December 2011, the General Services Administration, along with other Government bodies, established the Federal Risk Authorization Management Program (FedRAMP), a risk-based program designed to provide a standard, centralized approach to assessing cybersecurity controls and authorizing cloud computing services for operation. Federal agencies had until June 2014, to ensure that all new and existing cloud services met FedRAMP requirements.

In a prior Office of Inspector General (OIG) report on the *Department's Management of Cloud Computing Services* (OAS-RA-L-11-06, April 2011), we concluded that the Department of Energy had not developed policies and procedures governing security and other risks associated with cloud computing and had not adequately coordinated cloud computing efforts. A recent report by our colleagues at the National Aeronautics and Space Administration OIG, *NASA's Progress in Adopting Cloud-Computing Technologies* (Report No. IG-13-021, July 2013), identified weakness related to information technology governance, risk management practices and security requirements. As a result of issues identified during that audit, a Government-wide initiative was undertaken by the Council of Inspectors General for Integrity and Efficiency to provide insight to agency heads and lawmakers on how well the Federal government has adopted cloud computing technologies. In support of that effort, we initiated this audit to determine whether the Department efficiently and effectively managed its cloud computing environment.

RESULTS OF AUDIT

The Department had not always effectively or efficiently acquired, implemented or managed its cloud computing technologies. In particular, we found:

- Programs and sites independently acquired and managed cloud computing services valued at more than \$30 million. Despite the significant investment and number of programs/sites that utilized cloud services, the Department had not developed and maintained a complete inventory of cloud services to help manage its efforts. While the Office of the Chief Information Officer (OCIO) only reported 44 ongoing cloud initiatives to OMB, our testwork revealed that the Department had initiated at least 130 cloud computing efforts at 24 Federal and contractor locations. The lack of visibility into cloud computing efforts was not limited to the OCIO. We also found that program officials were often unaware of individual cloud computing efforts conducted at field offices and sites under their cognizance.
- The Department had not always established contracts with cloud computing service providers that ensured effective controls over the management of stored or transmitted information. Our review of eight contracts at six Federal and contractor locations found that contrary to Federal guidance and best practices, the contracts did not always address key business and cybersecurity risks. For instance, provisions/clauses permitting access to the cloud service provider's facilities, operations, documentation and databases by Department personnel were not incorporated into a majority of the contracts. This included the fact that, in many cases, the contracts did not allow for forensic investigations nor did they recognize the OIG's authority to access facilities to support audits and investigations.
- The Department had not ensured that cloud computing services were implemented in accordance with FedRAMP. While OMB required that agencies utilize cloud service providers that met the cybersecurity requirements of FedRAMP by June 2014, we found that none of the cloud services reviewed had fully implemented these requirements. Notably, three services were in the process of implementing all requirements and obtaining FedRAMP approval. The Department also incorrectly reported to OMB that the majority of cloud services met all FedRAMP requirements even though many of the services had not been approved – a key step in the FedRAMP process.

These issues occurred, in part, because the Department lacked a comprehensive strategy designed to ensure effective and efficient implementation of cloud computing technologies. In particular, programs and sites, including both Federal and contractor organizations, had not effectively coordinated efforts when implementing cloud computing initiatives. For instance, neither the OCIO nor the program offices had taken sufficient action to identify a comprehensive and accurate inventory of cloud computing services used across the complex. In addition, officials had not provided adequate oversight to ensure that programs and sites had taken appropriate action to acquire and implement cloud computing initiatives. In many cases, Federal officials had not ensured that programs and sites carried out their responsibilities for meeting FedRAMP requirements. Furthermore, programs and sites had not implemented risk management processes to ensure that critical oversight controls were in place related to access to facilities and data, establishment of service level agreements used to define acceptable levels of service, and ability to conduct audits and investigations related to cloud computing contracts.

Officials commented that cloud computing technology is highly dynamic and presents various risks. In addition, certain sites reported that they had realized cost savings through the

implementation of cloud computing services. However, without further improvement, the Department may not fully realize the potential benefits of adopting cloud computing technologies. For example, absent effective coordination between programs and sites, the Department may continue to expend more resources than necessary through the independent acquisition and implementation of cloud computing technologies. Moreover, moving systems and data into the cloud without an effective strategy, policy or adequate risk management practices can result in cloud computing technologies that fail to meet mission needs and key business or information technology security requirements.

While we recognize that there are challenges to implementing cloud computing services in a decentralized environment such as that which exists within the Department, we made recommendations that, if fully implemented, should help the Department manage its implementation of cloud technologies in a more secure and cost effective manner.

MANAGEMENT REACTION

Management concurred with the report's recommendations and indicated that it had initiated or planned corrective actions to address our recommendations. Management's comments and our response are summarized and more fully discussed in the body of the report. Management's formal comments are included in Appendix 3.

Attachment

cc: Deputy Secretary
Under Secretary for Nuclear Security
Deputy Under Secretary for Management and Performance
Deputy Under Secretary for Science and Energy
Chief of Staff
Chief Information Officer

AUDIT REPORT ON THE DEPARTMENT OF ENERGY'S MANAGEMENT OF CLOUD COMPUTING ACTIVITIES

TABLE OF CONTENTS

Audit Report

Details of Finding1

Recommendations6

Management Response and Auditor Comments7

Appendices

1. Objective, Scope and Methodology8

2. Related Reports10

3. Management Comments11

THE DEPARTMENT OF ENERGY'S MANAGEMENT OF CLOUD COMPUTING ACTIVITIES

DETAILS OF FINDING

While the Department of Energy (Department) had implemented numerous cloud computing initiatives in recent years, our review revealed that it had not always effectively or efficiently acquired, implemented or managed cloud computing services. We found that programs and sites were independently acquiring cloud computing services and providers and had not established an inventory of ongoing efforts. In addition, the Department had not always established contracts with cloud computing service providers that ensured effective controls over management of the Department's information. Furthermore, the Department had not ensured that cloud computing services utilized met the requirements of Federal Risk Authorization Management Program (FedRAMP). Due to the increased use of cloud computing initiatives throughout the Federal government, the Office of Management and Budget (OMB) directed that all agencies implement the FedRAMP to standardize the approach to system security and testing and reduce redundancy.

Inventory of Cloud Computing Services

When working to implement new information technology solutions, programs and sites were independently acquiring and managing cloud computing services and providers. We found that the Department entered into cloud computing contracts valued at more than \$30 million at numerous programs and sites. Despite the significance of the ongoing efforts, the Department had not developed and maintained a complete inventory of cloud computing services used by programs and sites. Specifically, while the Office of the Chief Information Officer (OCIO) reported that there were only 44 ongoing cloud initiatives, our test work revealed the Department had at least 130 initiatives underway at 24 Federal and contractor locations. OCIO officials told us that their information was based on responses to data calls submitted by programs to address OMB reporting requirements. However, based on the results of our review, we determined that the number of cloud computing initiatives reported by the Department to OMB was significantly understated.

Even within programs, officials were often unaware of individual cloud computing efforts conducted at their field offices and sites. For instance, Headquarters officials within the Office of Science (Science) were unaware of all cloud services acquired at sites and field offices, or which service providers were used. This was especially concerning because Science maintained the majority of cloud computing efforts within the Department. While management commented that many of the cloud computing efforts were still in the pilot and testing phase, our review focused only on those cloud systems that were operational. In response to our review, Science Headquarters and Argonne National Laboratory officials commented that they plan to leverage our results to maintain a program-level inventory of cloud services and providers. Oak Ridge National Laboratory also maintained an inaccurate inventory of service providers at the site. Specifically, contrary to documentation and officials' responses provided during our review, site officials told us near the end of our audit that one of their systems had been incorrectly reported to us as a cloud system. While the lack of an adequate inventory may have limited impact on the site's ability to manage security over cloud services, we are concerned that the inconsistent information provided by the site will further contribute to the inventory weaknesses identified within the Department. As noted in prior Office of Inspector General reports related to the

Department's unclassified cybersecurity program, maintaining an accurate and complete inventory of systems is needed to plan for and institute appropriate protective measures for systems, especially those that may contain sensitive and personally identifiable information.

Cloud Service Provider Contracts

The Department had not always established contracts with cloud computing service providers that ensured effective controls over the management of the Department's information. In support of a Government-wide review chartered by the Council of Inspectors General for Integrity and Efficiency, we examined a sample of the Department's cloud computing contracts to determine whether best practices for acquiring information technology as a service were met, as recommended by the Federal Chief Information Officers Council and the Chief Acquisition Officers Council.¹ In particular, our review of eight contracts at six Federal and contractor locations identified that the contracts did not address or mitigate key business and cybersecurity risks. For instance, contract clauses permitting access to the cloud service provider's facilities, operations, documentation and databases by Department personnel were not incorporated into a majority of the contracts reviewed. In addition, many of the contracts reviewed did not address the Department's ability to conduct forensic investigations, procedures for electronic discovery, or the Office of Inspector General's right to access facilities to support audits, inspections, investigations and other reviews. Specifically:

- One contract reviewed did not contain an executed service level agreement with the cloud service provider that defined acceptable service levels, provided performance metrics and outlined enforcement mechanisms. Officials at Argonne National Laboratory had not ensured that performance measures such as uptime percentages, service outages and remedies were specified within contract documentation. Absent such a control, programs and sites would have little or no recourse should the cloud service provider fail to perform as intended.
- A majority of the cloud contracts reviewed lacked required and/or recommended practices, such as those in Federal Acquisition Regulations. In particular, seven of eight contracts reviewed omitted language permitting the Office of Inspector General access to pertinent cloud service records or the ability to interview cloud service personnel regarding Department related transactions.
- An ongoing review at the Bonneville Power Administration revealed weaknesses related to the site's procurement contract for a recruiting/human resource cloud service provider. Preliminary test work identified that Bonneville Power Administration's contract with the cloud service provider had not included several mandatory clauses and/or best practices such as those related to data ownership rights, inspection, and acceptance. As a result, Bonneville Power Administration exposed itself to unnecessary risk.

While we recognize that there are various contracting implications to consider when evaluating cloud computing technologies, the purpose of the Government-wide Council of Inspectors

¹ Creating Effective Cloud Computing Contracts for the Federal Government: *Best Practices for Acquiring IT as a Service*, February 24, 2012.

General for Integrity and Efficiency review was to, among other things, evaluate contracts between agencies and cloud service providers to determine whether applicable standards and best practices had been appropriately implemented.

FedRAMP Implementation

The Department had not ensured that cloud computing providers utilized by programs and sites met the requirements of FedRAMP. FedRAMP was established in 2011, by the General Services Administration, along with other Government bodies, to provide a cost-effective, risk-based approach for the adoption and use of cloud services by making available a "do once, use many times" approach. Although OMB required that agencies' cloud service providers must be compliant with FedRAMP by June 2014, we found that various cloud providers reviewed were not approved and/or had not begun the FedRAMP approval process, to include submission of security documentation to FedRAMP.

While officials told us that certain cloud services were in the process of becoming approved, none of the cloud services reviewed had yet obtained FedRAMP approval to ensure that security authorizations could be leveraged Government-wide. In addition, we determined that none of the contracts reviewed required approval by the deadline. We found that only one cloud service provider used by several sites reviewed had submitted security assessment packages to FedRAMP for inclusion in the repository – a process designed to reduce the burden of duplicative security testing by other organizations. As a result, the lack of implementation may limit the Department's ability to realize reduced procurement and operating costs related to assessing FedRAMP security controls.

We also found that the Department did not accurately report progress as part of its quarterly submissions to OMB. Specifically, based on the OCIO's data call instructions, Department elements reported that 30 of 44 cloud initiatives met FedRAMP requirements even though the services had not fully implemented requirements and been approved by FedRAMP authorities. Although one site reported that all 20 of its cloud computing services were compliant with FedRAMP, we found no evidence that the services had been approved, which could have allowed other organizations to eliminate duplicative testing of the same cloud services. Similarly, while the OCIO noted that one of its cloud service providers was approved, we found that the provider had only initiated the process and had yet to be designated FedRAMP compliant. Furthermore, for those services that were not approved, the Department did not identify and report planned corrective actions to OMB, as required. Absent approval of cloud computing services, the Department may not meet FedRAMP's primary objective of providing a cost-effective, risk-based approach to cloud services by leveraging cloud service assessment and authorization activities.

Cloud Computing Strategy

The issues we identified occurred, in part, because the Department lacked a comprehensive strategy designed to ensure effective and efficient implementation of cloud computing technology. In particular, programs and sites had not effectively coordinated efforts when implementing cloud computing initiatives. Officials also had not provided adequate performance

monitoring to ensure that programs and sites had taken appropriate action to effectively acquire and implement cloud computing initiatives. In addition, programs and sites had not adequately implemented risk management processes to ensure that critical oversight controls over cloud service providers were in place.

Coordination

Department programs and sites, including both Federal and contractor organizations, had not effectively coordinated efforts when implementing cloud computing initiatives. For instance, neither the OCIO nor the program offices had taken sufficient action to identify a comprehensive and accurate inventory of cloud computing services in use across the complex. Such an inventory could have helped establish a baseline architecture and potentially eliminated duplication by leveraging cloud acquisition efforts. Although the OCIO issued a request to programs and sites to determine the number of cloud initiatives throughout the Department, responses to the data call were, in many cases, nonexistent. Even when responses were provided, we found that the OCIO had not taken action to validate the results prior to reporting cloud computing information to OMB. In addition, although the Department developed documents such as the *Department of Energy National Laboratories and Plants Leadership in Cloud Computing* and the *Fiscal Years 2014-2018 Information Resources Management Strategic Plan*, we found that these documents did not address elements such as FedRAMP requirements and/or coordination of programmatic and site cloud computing efforts.

Notably, we observed positive actions designed to increase collaboration among national laboratories and decrease the time spent on contract negotiations. In one case, a blanket purchase agreement for a cloud service was negotiated by Lawrence Berkeley National Laboratory on behalf of several of the Department's programs and sites. Officials told us that the agreement included favorable pricing terms that provided the opportunity to decrease the per user license cost as more customers subscribe to the service.

Oversight and Risk Management

Officials had not ensured that programs and sites had taken appropriate action to effectively acquire and implement cloud computing services. For instance, contrary to industry best practices, Department officials had not established policies and procedures to ensure that implementation of cloud computing initiatives included common considerations such as information security risks related to privacy, compliance, data location, certification and records management. We also found that no guidance existed related to areas such as service level agreements, auditing and end-user roles and responsibilities. Although the OCIO developed the *DOE Cloud Computing Toolkit*, in September 2012, to provide limited cloud computing guidance, the document does not carry the force of mandate to assist Department officials with developing a policy framework, ensuring appropriate coordination or setting strategy based on risks in alignment with the Department's enterprise architecture. Further, many program and site officials did not know the toolkit existed or did not utilize the document. Notably, management commented that its cloud computing requirements for the Office of Energy Information Technology Services exceeded FedRAMP requirements in certain instances, such as in the case of establishing the trustworthiness of foreign nationals.

Officials also had not ensured that programs and sites, including management and operating contractors, carried out their responsibilities for meeting FedRAMP requirements. For example, management and operating contractor officials commented that they were not required to comply with FedRAMP. As such, sites were not working with cloud service providers to update contractual requirements or identify actions needed to address the requirements of FedRAMP for each service. A Science Headquarters official commented that without Department policy, it was difficult to enforce the requirements on contractors. However, an OMB memorandum on *Security Authorization of Information Systems in Cloud Computing* dictated that FedRAMP policy is applicable to information systems that support operations and assets of the Department, including those systems provided or managed by other agencies or contractors. These issues were exacerbated by incorrect interpretation of FedRAMP policy by programs and sites, including certain elements of the OCIO. While OCIO officials stated that FedRAMP policy required that a Federal cloud service be compliant with security controls established by the National Institute of Standards and Technology, they asserted that services were not required to be certified as a cloud service provider through the FedRAMP process. However, FedRAMP officials stated that cloud service providers must be both compliant with FedRAMP security controls and approved by FedRAMP authorities.

We also found that programs and sites had not implemented risk management processes to ensure that critical oversight controls were in place related to access to facilities and data, establishment of service level agreements and the ability to conduct audits and investigations. For example, while Argonne National Laboratory officials stated that they had discussed the risk of moving information into the cloud with Federal officials who accepted the risk as part of the Laboratory's overall risk management process, we found that items such as a risk assessment and related mitigating controls were not documented or approved, as appropriate. To its credit, Idaho National Laboratory worked extensively with its authorizing official to ensure that key business and cybersecurity risks were evaluated and mitigated as necessary within cloud contract provisions prior to placing the service in operation. According to the National Institute of Standards and Technology, placing Federal systems and data into a public cloud poses challenges because the computing environment is under the control of the cloud service provider rather than the Department. As such, effective risk management requires establishing contracts that address how a contractor's performance will be managed and how cybersecurity, privacy and information management requirements will be met.

Opportunities for Improvement

Without improvements, the Department may not fully realize the potential benefits of adopting cloud computing technologies, including improved information technology service delivery, increased collaboration and potential cost reductions. In addition, absent effective coordination between programs and sites, the Department may spend more resources than necessary independently acquiring and implementing cloud computing technologies. Transitioning to cloud computing services without an effective strategy, policy or adequate risk management practices can result in cloud computing technologies that fail to meet mission needs and key business or information technology security requirements. Ultimately, the availability, integrity and confidentiality of Federal systems and data may be placed at an unnecessarily high risk. Furthermore, continuing on a path of non-compliance with FedRAMP requirements may prevent the Department and its contractors from effectively leveraging ongoing initiatives, resulting in duplicative efforts and resources related to implementing security processes and controls.

RECOMMENDATIONS

To improve the management and coordination of cloud computing activities, we recommend that the Under Secretary for Nuclear Security, the Deputy Under Secretary for Management and Performance and the Deputy Under Secretary for Science and Energy, in coordination with the Department's and National Nuclear Security Administration's Chief Information Officers:

1. Establish a cloud computing strategy in accordance with FedRAMP requirements that includes effective coordination of programmatic and site efforts and development of an inventory of cloud computing services.
2. Ensure effective oversight over cloud computing efforts, including development and implementation of policies and/or procedures related to the acquisition, implementation and security of cloud computing services that:
 - a. Ensures contracts with cloud service providers include, among other things, language related to service level agreements, auditing and roles and responsibilities;
 - b. Clarifies discrepancies between the Office of the Chief Information Officer and FedRAMP related to approval of the Department's cloud service providers in accordance with Federal requirements; and
 - c. Provides direction ensuring that the Department and its management and operating contractors implement systems in accordance with applicable FedRAMP requirements.
3. Ensure key business and security risks related to implementation of cloud computing services are adequately evaluated, mitigated and documented.

MANAGEMENT RESPONSE

Management concurred with each of the report's recommendations and indicated that corrective actions were initiated or planned to address the issues identified. For example, the Department established an Information Management Governance Board that will be leveraged to align and communicate cloud strategy and requirements to support the Department's mission and objectives. In addition, management commented that the Department will continue to develop, evaluate and revise guidance regarding service level agreements, auditing and roles and responsibilities, including the use of standard contractual clauses. Management also indicated that the Department is working with the FedRAMP Program Management Office to clarify the requirements for FedRAMP compliance and approval for the Department's cloud computing services.

AUDITOR COMMENTS

Management's comments and planned corrective actions were responsive to our recommendations. Management's comments are included in Appendix 3.

OBJECTIVE, SCOPE AND METHODOLOGY

Objective

The objective of this audit was to determine whether the Department of Energy (Department) efficiently and effectively managed its cloud computing environment.

Scope

The audit was performed between January and September 2014, at Department Headquarters in Washington, DC and Germantown, Maryland; the Argonne National Laboratory in Argonne, Illinois; the Fermi National Accelerator Laboratory in Batavia, Illinois; the Idaho National Laboratory in Idaho Falls, Idaho; the Lawrence Berkeley National Laboratory in Berkeley, California, and the Oak Ridge National Laboratory in Oak Ridge, Tennessee. We reviewed cloud computing activities for various program offices, including the Offices of Nuclear Energy, Science, Fossil Energy, Environmental Management, the Chief Information Officer, as well as the National Nuclear Security Administration. The audit was conducted under Office of Inspector General Project Number A14TG017.

Methodology

To accomplish our objective, we:

- Reviewed applicable laws, regulations and directives related to cloud computing.
- Reviewed relevant reports issued by the Office of Inspector General and the Government Accountability Office.
- Reviewed best practices and Office of Management and Budget memoranda pertaining to cloud computing activities such as the Federal Risk and Authorization Management Program.
- Judgmentally selected a sample of cloud services for a detailed review. We selected eight services from cloud computing initiative surveys that were completed by the Department's program offices. Our selection criteria included the cost of the service, number of users and whether the service had been placed into production.
- Reviewed relevant documentation such as cloud contracts, terms of service, service level agreements and non-disclosure agreements.
- Held discussions with field site officials and officials from various Departmental offices responsible for cloud computing activities and cloud acquisition and contracting.

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 objective. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Accordingly, we assessed significant internal controls and compliance with laws and regulations to the extent necessary to satisfy the audit objective. In particular, we assessed the Department's implementation of the *GPRA Modernization Act of 2010*. Although the Department had established certain overarching performance goals subsequent to our audit work, none of the sites evaluated had established performance metrics specific to the acquisition and use of cloud computing services. Because our review was limited, it would not necessarily have disclosed all internal control deficiencies that may have existed at the time of our audit. We did not rely on computer-processed data to satisfy our audit objective.

An exit conference was held with Department management on September 12, 2014.

RELATED REPORTS

Office of Inspector General

- Audit Report on the [*Department's Management of Cloud Computing Services*](#), (OAS-RA-L-11-06, April 2011). The report identified areas that the Department of Energy (Department) should consider before it moves forward with adopting such cloud computing technology on a large scale. Specifically, we noted several opportunities for improvement in the Department's cloud computing initiatives. For instance, the Department had not yet prepared policies and procedures governing security and other risks or established coordination requirements among sites to prevent duplication or other problems with cloud computing initiatives.

Government Accountability Office

- Report on the [*Progress Made but Future Cloud Computing Efforts Should be Better Planned*](#), (GAO-12-756, July 2012). The report stated that selected Federal agencies have made progress implementing the Office of Management and Budget's "Cloud First" Policy. Consistent with this policy, each of the seven agencies incorporated cloud computing requirements into their policies and processes. During the review, the Government Accountability Office identified seven common challenges associated with the implementation of Office of Management and Budget's "Cloud First" Policy, including acquiring knowledge and expertise, as well as certifying and accrediting vendors.
- Report on [*Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing*](#), (GAO-10-513, May 2010). According to the report, cloud computing can both increase and decrease the security of information systems in Federal agencies. As such, Federal agencies had begun efforts to address information security issues for cloud computing, but key guidance was lacking and efforts remained incomplete. Although individual agencies identified security measures needed when using cloud computing, they had not always developed corresponding guidance. For example, only nine agencies had approved and documented policies and procedures for writing comprehensive agreements with vendors when using cloud computing.

National Aeronautics and Space Administration

- Audit Report on [*NASA's Progress in Adopting Cloud-Computing Technologies*](#) (Report No. IG-13-021, July 2013). The National Aeronautics and Space Administration's (NASA) information technology governance and risk management practices impeded the Agency from fully realizing the benefits of cloud computing and potentially put systems and data stored in the cloud at risk. For example, NASA officials moved systems and data into public clouds without the knowledge or consent of the Agency's Office of the Chief Information Officer. Moreover, on five occasions, NASA acquired cloud-computing services using contracts that failed to fully address the business and information technology security risks unique to the cloud environment.

MANAGEMENT COMMENTS



Department of Energy

Washington, DC 20585

August 18, 2014

MEMORANDUM FOR RICKEY HASS

DEPUTY INSPECTOR GENERAL
FOR AUDITS AND INSPECTIONS
OFFICE OF INSPECTOR GENERAL

FROM:

ROBERT F. BRESE 
CHIEF INFORMATION OFFICER

SUBJECT:

Draft Report, "The Department of Energy's Management of
Cloud Computing Activities" (A14TG017)

Thank you for the opportunity to comment on the subject draft report. The Department recognizes that the Inspector General's (IG) objective in this review was to participate in an overall a Government-wide initiative, undertaken by the Council of Inspectors General for Integrity and Efficiency, to provide insight to agency heads and lawmakers on how well the Federal government has adopted cloud computing technologies.

In support of that effort, we have worked to support this audit to review the efficiency and effective management of the Department's cloud computing environments. We appreciate the IG's efforts to review Department-wide activities and we agree with the IG's assertion that there is significant potential to reduce the cost of Federal information technology systems, while improving capabilities and stimulating innovation in information technology solutions, by strengthening the coordination of our cloud computing and overall technology efforts.

The management response to the recommendations identified in the draft report is outlined below. More specific feedback and direct Program comments are included in the attachments.

Recommendation 1: *Establish a cloud computing strategy in accordance with FedRAMP requirements that includes effective coordination of programmatic and site efforts and development of an inventory of cloud computing services.*

Management Response: Concur.

The Department's Information Resource Management (IRM) vision is to collaborate as an enterprise to deliver innovative management and technology solutions that support the Department's mission. The FY 2014-2018 IRM Strategic Plan addresses this recommendation through Objective 1.2 to "Create new capacity through a network of Department of Energy (DOE) clouds that will achieve enhanced performance of information and IT solutions by integrating networks and services."



Printed with soy ink on recycled paper

Prior to the FY 2014-2018 DOE IRM Strategic Plan, the Department had more than 15 strategic documents that attempted to guide DOE information technology (IT) and IRM efforts. The DOE IRM Strategic Plan was signed by the Deputy Secretary and the Chief Information Officer with an acknowledgement that: "Active participation and commitment will be required from all Departmental Elements" and that unification under a single IRM Strategic Plan was critical to enabling the Department to "meet and exceed the rising expectations of our stakeholders, business partners, and the information consumers that we serve."

Additionally, the Department has established an Information Management Governance Board (IMGB), which along with Enterprise Architecture (EA) and Capital Planning and Investment Control (CPIC) activities, will be leveraged to align and communicate cloud strategy and requirements to support DOE's mission and objectives.

Estimated Completion Date: September 30, 2015.

Recommendation 2: *Ensure effective oversight over cloud computing efforts, including development and implementation of policies and/or procedures related to the acquisition, implementation and security of cloud computing services that:*

Management Response: Concur.

The security of cloud-based systems, indeed all DOE information systems, is guided by the overarching requirements codified in DOE Order (O) 205.1B, *Department of Energy Cyber Security Program*. The directive establishes requirements and responsibilities for DOE's federated cybersecurity model in which Under Secretary-level organizations tailor cybersecurity requirements for their operating units based on mission requirements. While the Order is not comprehensive in detailing mandatory cybersecurity controls, it requires compliance with statutory requirements and identifies how the Department will adhere to Federally mandated programs (e.g., those of the Committee on National Security Systems [CNSS], the Office of Management and Budget [OMB], and the Department of Homeland Security [DHS]), whether or not they are specifically delineated in the Order. Through updates to DOE O 205.1B, the Department will ensure there are clear requirements and guidance regarding oversight of cloud computing efforts.

Recommendation 2.a: *Ensures contracts with cloud service providers include, among other things, language related to service level agreements, auditing and roles and responsibilities;*

Management Response: Concur.

The Department currently leverages federal contracting guidance in all IT procurement activities. Heads of Departmental Programs and mission elements and DOE Contracting Officials are responsible for working with the DOE Office of Management, Office of Acquisition and Project Management (OAPM) and the NNSA Office of Acquisitions and Supply Management (OASM) in providing procurement policy and guidance to contracting officers and contractors and incorporating departmental requirements into all

contracting and acquisition activities; and to ensure contractor compliance with all Departmental requirements during performance.

The Department will continue to develop, evaluate and revise guidance regarding service level agreements, auditing and roles and responsibilities, including the use of standard contractual clauses. The CIO will work with the Federal CIO Council, as well, to leverage operating experiences and best practices of other agencies.

Estimated Completion Date: September 30, 2015.

Recommendation 2.b: *Clarifies discrepancies between the Office of the Chief Information Officer and FedRAMP related to approval of the Department's cloud service providers in accordance with Federal requirements; and*

Management Response: Concur.

The Office of Cyber Security is working with the FedRAMP Program Management Office to clarify the requirements for FedRAMP compliance and approval for DOE cloud-based systems. The results of this discussion will be considered in the evaluation process for developing DOE-specific FedRAMP requirements to be included in a planned revision of DOE O 205.1B and any other supplemental guidance.

Recommendation 2.c: *Provides direction ensuring that the Department's management and operating contractors implement systems in accordance with applicable FedRAMP requirements.*

Management Response: Concur, with comment.

DOE O 205.1B requires Under Secretary-level organizations to specify cybersecurity requirements, including implementation of federal policy, for their operating units (including management and operating contractors), in organizationally tailored cybersecurity programs. If direct compliance with policy is not in the best interest of the mission, the Under Secretary may tailor the implementation and inform the CIO. The CIO will work with the Under Secretary to ensure the implementation strategy is defensible from an outcome-based perspective and, where necessary, communicate the implementation to DHS.

Estimated Completion Date for Recommendations 2b and 2c: September 30, 2015.

Recommendation 3: *Ensure key business and security risks related to implementation of cloud computing services are adequately evaluated, mitigated and documented.*

Management Response: Concur.

DOE O 205.1B requires Under Secretary-level organizations to specify cybersecurity requirements, including implementation of federal policy, for their operating units (including management and operating contractors), in organizationally tailored

cybersecurity programs. The responsibility for oversight of the implementation of such programs and risk assessment and management at the operating unit level also resides with the Under Secretary organizations, either as part of system authorization processes, contractor assurance in accordance with the DOE Oversight Policy, DOE P 226.1, or other management reviews. The Department will continue to work to ensure cloud computing services are adequately evaluated, mitigated and documented, and update DOE O 205.1B, to reflect this recommendation as part of a planned upcoming revision.

Estimated Completion Date: September 30, 2015.

Attachments

1. Program-specific Comments for Consideration
2. Technical Comments for Consideration
3. DOE Site Comments for Consideration

FEEDBACK

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We aim to make our reports as responsive as possible and ask you to consider sharing your thoughts with us.

Please send your comments, suggestions and feedback to OIGReports@hq.doe.gov and include your name, contact information and the report number. Comments may also be mailed to:

Office of Inspector General (IG-12)
Department of Energy
Washington, DC 20585

If you want to discuss this report or your comments with a member of the Office of Inspector General staff, please contact our office at (202) 253-2162.