Office of Inspector General

OFFICE OF CYBER ASSESSMENTS AND DATA ANALYTICS

AUDIT REPORT

SECURITY OVER CLOUD COMPUTING TECHNOLOGIES AT SELECT DEPARTMENT OF ENERGY LOCATIONS

DOE-OIG-23-18
MARCH 2023

Department of Energy
Washington, DC 20585

March 30, 2023

MEMORANDUM FOR THE SECRETARY

SUBJECT: Audit Report on Security over Cloud Computing Technologies at Select Department of Energy Locations

The attached report discusses our review of whether the Department of Energy effectively implemented security measures over its cloud-based technologies and services in accordance with Federal and Department requirements. This report contains six recommendations that, if fully implemented, should improve the Department's ability to secure its cloud-based systems. The recommendations are designed to ensure that all cloud-based systems contain appropriate security controls, that security controls are adequately monitored, and that cloud-based systems are appropriately approved for operation. Management concurred with Recommendations 1 through 5. Management did not concur with Recommendation 6. However, based on additional information provided by the Department, we consider Recommendation 6 closed. We also consider Recommendation 1 closed for the National Nuclear Security Administration based on corrective actions taken. Recommendation 1 remains open for the Under Secretary for Science and Innovation.

We conducted this audit from January 2021 through December 2022 in accordance with generally accepted government auditing standards. We appreciate the cooperation of your staff during the review.

Teri L. Donaldson

Teri L. Donaldson
Inspector General

cc: Deputy Secretary
Chief of Staff
Under Secretary for Science and Innovation
Chief Information Officer

Department of Energy
Office of Inspector General

Security over Cloud Computing Technologies at Select Department of Energy Locations
(DOE-OIG-23-18)

WHY THE OIG PERFORMED THIS REVIEW

The Department of Energy has significantly increased its adoption of cloud-based systems in recent years. The transition to cloud-based services shifts some responsibility and risk to the cloud service provider. However, the Department remains obligated to ensure the confidentiality, integrity, and availability of its data by identifying and accepting the risk of utilizing cloud service providers and authorizing the operation of such services.

We initiated this audit to determine whether the Department effectively implemented security over its cloud-based technologies and services.

What Did the OIG Find?

Although the Department had implemented security measures over many of its cloud-based technologies and services, additional efforts are necessary. Specifically, we found weaknesses with the Department's processes to authorize, monitor, assess, control, and inventory cloud-based services used by its programs and sites. In particular:

- Two locations utilized cloud-based systems without appropriate approval. Additionally, three locations had not conducted complete system authorizations for cloud systems, to include identifying, implementing, and assessing security controls for which the Department was responsible.
- Three locations had not conducted required continuous security monitoring of cloud services that were authorized through the Federal Risk and Authorization Management Program.
- Significant amounts of information were stored in unapproved cloud storage accounts.
- The Department did not maintain an accurate inventory of cloud-based systems used across the enterprise, and programs and sites generally used more systems than were reported to the Office of the Chief Information Officer.

What Is the Impact?

Without improvements, the Department may not be adequately protected from the risks posed by the use of systems outside its physical network boundaries, such as unauthorized access and data exfiltration.

What Is the Path Forward?

To address the weaknesses identified during our review, we made six recommendations in this report designed to ensure that all cloud-based systems contain appropriate security controls, that security controls are adequately monitored, and that cloud-based systems are appropriately approved for operation.

Table of Contents

Background and Objective

Background

Cloud computing[1] systems and services provide significant benefits to the Department of Energy. For example, cloud system implementations have helped the Department meet Federal requirements to reduce data center costs and replace legacy information technology that is more susceptible to malicious cyber activity because it is outdated or obsolete. We have previously reported on the Department's efforts to implement cloud systems. Most recently, our audit report, *The Department of Energy's Management of Cloud Computing Activities* (DOE/IG-0918, September 2014), found issues with the Department's development and maintenance of a complete inventory of cloud systems and noted that the Department had not ensured cloud computing services were implemented in accordance with the Federal Risk Authorization Management Program (FedRAMP).[2] In response to that report, the Department planned to update strategic plans and working groups, work with the FedRAMP Program Management Office to clarify requirements, and ensure requirements associated with the Department's cybersecurity directive were implemented.

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations*, outlines a repeatable process for Federal agencies to use to promote the protection of information and information systems commensurate with risk. It requires that the authorization to use a system must be granted by an Authorizing Official,[3] based on the results of system assessments. Additionally, NIST notes that the Risk Management Framework is technology-neutral and provides a dynamic and flexible approach to effectively manage security and privacy risks in diverse environments, including cloud-based systems.

FedRAMP is a Government-wide program that provides a standardized approach to implementing the Risk Management Framework for products and services from cloud service providers. FedRAMP provides a "do once, use many times" approach that reduces the cost, time, and labor required for security assessments and authorizations by allowing agencies to share a single authorization for a cloud system. To maintain FedRAMP certification, a cloud

[1] As defined by NIST SP 800-145, *The NIST Definition of Cloud Computing*, "cloud computing" is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

[2] FedRAMP is a Government-wide program that promotes the adoption of secure cloud services across the Federal Government by providing a standardized approach to security and risk assessment for cloud technologies and Federal agencies. It enables the Federal Government to accelerate the adoption of cloud computing by creating transparent standards and processes for security authorizations and allowing agencies to leverage security authorizations on a Government-wide scale.

[3] The Authorizing Official is a senior Federal official or executive with the authority to authorize (i.e., assume responsibility for) the operation of an information system or the use of a designated set of common controls at an acceptable level of risk to agency operations, assets, and individuals. Agencies are not required to develop a separate risk management process for cloud-based systems.

service provider must agree to make certain deliverables associated with continuous monitoring[4] available to agencies that have authorized the service for use. For example, cloud service providers must provide monthly vulnerability scanning reports for operating systems, web applications, and databases and plan of actions and milestones status updates. Further, cloud service providers must provide evidence that all discovered high-risk vulnerabilities are mitigated within 30 days, moderate-risk vulnerabilities within 90 days, and low-risk vulnerabilities within 180 days. Federal agencies that authorize the system can be granted permanent access to this information and incorporate it into their continuous monitoring processes to support the system's ongoing authorization.

In May 2021, the President issued an Executive Order, *Improving the Nation's Cybersecurity,* which acknowledged that the Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to persistent and increasingly malicious cyber threats. One area the Executive Order identified for improvement was modernizing Federal Government cybersecurity through accelerated movement to secure cloud services. Federal agencies were required to update their plans to prioritize resources for the adoption and use of cloud technology.

Report Objective

The objective of this audit was to determine whether the Department effectively implemented security over its cloud-based technologies and services.

[4] NIST SP 800-37, NIST SP 800-53 Revision 4, *Security and Privacy Controls for Information Systems and Organizations*, and NIST SP 800-137, *Information Systems Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, require continuous monitoring and ongoing assessments of security controls for Federal information systems.

Results of Review

Since our prior report, the Department has substantially increased the number of cloud computing systems in use to support various functions such as email, file sharing, and information technology service management. We reviewed 5 locations that reported using 227 cloud systems and selected 17 cloud systems to review in detail. Based on our test work, we determined that issues related to cybersecurity over these selected systems continue to persist. Specifically, we found weaknesses related to the Department's processes to authorize, monitor, assess, control, and inventory the cloud-based systems used by its programs and sites.

Cloud Computing Systems Authorization

Two locations reviewed used cloud-based systems that had not received approval to operate from the site's Authorizing Official. Specifically, we found that one location's Authorizing Official had not approved all of the cloud-based systems used by the site. Instead, site cybersecurity procedures outlined a "Rapid Risk Assessment" approach that permitted the contractor to authorize cloud-based systems to operate without undergoing a formal system authorization process as long as each system was utilized by fewer than 100 users and contained no controlled unclassified information. At the time of our review, approximately 120 cloud-based systems or services had undergone the "Rapid Risk Assessment" process at the site. However, this approach circumvented the NIST requirement for explicit approval and risk acceptance by the Authorizing Official. Site officials stated that cloud-based systems approved through the "Rapid Risk Assessment" process were included in the site's annual *Cybersecurity Cloud Services System Assessment Report* that was submitted to the Authorizing Official. However, we noted that this assessment was completed after cloud systems were put into service by the site's contractor. The annual assessment report also resulted in two contractor-approved systems being deemed too risky and blocked from future use.

We identified concerns with some of these cloud-based systems that could have introduced a higher level of risk to the site that the Authorizing Official was unaware of and had not explicitly accepted. For example:

- The site implemented a cloud-based collaboration tool that permitted many capabilities such as uploading files and sharing of workspaces. However, if not properly configured, workspace sharing could make information publicly visible to anyone on the internet and appear in internet search engines. In January 2020, Sophos—a cybersecurity firm—reported the results of vulnerabilities it identified associated with the service, which included exposure of staff performance ratings, names, emails, dates of birth, identification numbers, bank account information, and passwords and credentials stored in the cloud system that were accessible to anyone on the internet using simple Google searches. The information identified was not affiliated with the site. However, Sophos noted that due to legacy settings for the system, a user could make information public, mistakenly believing that the setting was necessary to share with a private group. Further, users could upload information to a board without realizing that it was public.

- The same site also implemented a cloud-based video conferencing tool that had many security and privacy problems, including a settlement with the Federal Trade Commission because the cloud service provider deceptively advertised that it had end-to-end encryption when it did not. Additionally, the cloud system had serious security issues with malware embedded software installers, foreign influence, and hacking flaws. The Department's Office of the Chief Information Officer (OCIO) conducted an inherent risk analysis for the cloud system and identified potential issues that could allow malicious scripts to be injected by attackers, man-in-the-middle[5] attacks, and distributed denial of service attacks. Although the tool was FedRAMP authorized, the site's process did not include review of that information to identify any potential risks.

Similarly, a second site operated two cloud computing systems without approval from the Authorizing Official. In these instances, contractor officials maintained that the systems did not contain data that would require Federal authorization. Like the cloud systems at the first site, these systems had not undergone a controls identification and assessment process, and the Authorizing Official had not explicitly accepted the risk associated with their operation. These cloud systems also had security concerns. One system collected personally identifiable information from potential job candidates, while another system, used for communications with the board of managers, contained "official use only" information without having gone through a security review or formal approval. The Department's Office of Enterprise Assessments reported on the lack of Federal authorization in a 2021 report to the site. At the time of our review, site officials told the audit team that the cloud system associated with its executives had been scoured of all Federal data and continued to operate with only corporate, contractor data. Site officials also advised that the job candidate cloud system continued to operate as it had previously and would be phased out by a new federally authorized system in the future. However, this was not completed at the time of our review.

FedRAMP Continuous Monitoring

Although all five locations reviewed leveraged FedRAMP certified systems, we found that officials at three of the locations had not conducted the required continuous monitoring to support systems' ongoing authorizations. Despite having authorized several cloud systems through FedRAMP, two locations did not regularly review monitoring reports prepared by the cloud service providers, and three locations had not defined in their continuous monitoring plans and procedures the need to review these reports or the frequency with which they should be reviewed.

Program officials at one location stated that their cloud systems were sponsored and authorized by another Department element or Federal agency and that the authorizing entity was monitoring security controls and plans of actions and milestones. However, these cloud systems were on the location's network, and certain vulnerabilities were identified with cloud systems specific to that network. FedRAMP documentation required that each user entity authorize cloud solutions within the context of their own organizations and risk tolerances. In addition, FedRAMP noted that solely relying on other agency authorizations could increase risk if the initial authorizing

[5] A man-in-the-middle attack is where an adversary is positioned in between the user and the system to intercept and alter data traveling between them.

agency were to discontinue use of the product and no longer monitor it. Even though the location reviewed had identified multiple significant deficiencies for some of its cloud systems in risk assessments, program officials had not utilized the information available through FedRAMP to monitor those deficiencies and identify any impact on the risk to the organization. In particular, program officials had not updated risk assessments for three of five cloud systems reviewed even though, in some cases, assessments had not been conducted in over 5 years. For example, a 2017 risk assessment completed by the site identified 112 high-risk weaknesses related to an office productivity service's flaw remediation control. According to that assessment, high-risk threats required a corrective action plan to be put in place as soon as possible. However, a corrective action plan was not created. Program officials stated that they relied on the FedRAMP sponsoring entity to monitor the status and remediation of weaknesses. As a result, no monitoring of the service's weaknesses had been performed since the initial risk assessment, and program officials were unaware of their status at the time of our audit. Similarly, multiple vulnerability scanning weaknesses were identified and not monitored in 2016 on a file sharing platform and in 2019 on a cybersecurity product. As a result of our review, an official stated that the site planned to develop a process to review FedRAMP monitoring reports to determine the status of weaknesses and whether any updates had occurred.

In addition, the site that had implemented the "Rapid Risk Assessment" had not implemented a continuous monitoring process on the systems and services that received authorization through that process. Continuous monitoring is designed to assess control effectiveness on an ongoing basis and ensure critical information contained in authorization documentation is kept up-to-date to maintain authorization decisions. It appeared that several of the contractor-approved cloud systems were also FedRAMP-authorized, which could have allowed site officials to monitor those systems for vulnerabilities and the status of service provider-implemented security controls. However, the site did not use FedRAMP to support system authorization and continuous monitoring. Instead, the site utilized a Cloud Access Security Broker[6] that assigned a risk score for individual cloud systems. Although the risk scores were updated frequently, they were not as robust as a comprehensive continuous monitoring program. As a result of our audit work, in July 2021, the site's Federal oversight office expressed concerns with the process and had initiated discussions with the site contractor regarding potential changes and improvements.

Due to the Department's lack of control over its information when stored in cloud-based systems, regular review of security monitoring information is a critical activity to ensure Authorizing Officials remain aware of a system's risk posture. Obtaining and reviewing continuous monitoring reports from FedRAMP could enable user entities to identify these changes in a timely manner and report them to the Authorizing Official to ensure that the service continues to operate within the site's risk tolerance. For example, one cloud system used at four of the sites reviewed related to information technology support had increased from a moderate- to a high-impact categorization, which required implementation of significantly more security controls. However, program and site officials at two of the locations were unaware of the system's categorization change and, therefore, had not considered the impact to the organizations' security postures.

[6] Cloud access security brokers are on-premises, or cloud-based security policy enforcement points, placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as the cloud-based resources are accessed.

Security Control Assessments

Three of the five locations reviewed had not performed security control assessments[7] on cloud-based systems, as required. The FedRAMP process requires cloud service providers to submit a control implementation summary workbook, which includes a customer responsibility matrix listing controls that must be implemented by the cloud service provider, the customer, or have shared implementation responsibility. It is the Department's responsibility to ensure that customer and shared controls are fully implemented on all cloud-based systems to minimize the risk to the Department's information. Contrary to this requirement, two locations reviewed had not conducted the analyses to determine security controls for which they were responsible nor had they conducted assessments to ensure the controls were implemented and operating as intended. At one of the locations, site officials stated that they considered cloud service provider documentation as an administrative guide and had not performed a detailed analysis of security controls for which they were responsible. During our audit, officials at that location stated that they would develop a procedure for conducting a detailed security controls analysis on their cloud systems. At the second location, program officials stated that they had conducted Security Assessment Reports for cloud systems. However, as noted earlier, three of these controls assessments had not been updated in over 5 years, and identified deficiencies from those assessments had not been corrected. The third location had not assessed the implementation of security controls for one of the two cloud systems we selected for review at the site even though the system was approved for operation in 2016. Site officials stated that they concluded that all security controls were operating as intended, and risks were identified prior to implementation. When notified of our preliminary findings, site officials stated that the control assessment was in process and expected it to be complete by the end of 2021. However, due to system changes and delays related to COVID-19, the assessment was delayed until at least May 2022. As a result, none of the three locations were aware of whether security controls were operating as intended and had not identified the risks associated with utilizing the systems.

Notably, the two other sites we reviewed had obtained customer responsibility matrices, analyzed controls for which the Department was responsible, and ensured that they were implemented. While this is encouraging, additional action is needed to ensure that all of the Department's cloud system users implement consistent processes to assess whether controls are appropriately implemented on cloud-based systems and services and use those results to inform each system's authorization.

Unmanaged Cloud Systems

The Department had not ensured that only approved cloud services were used to store its information. In particular, we identified a significant amount of information stored in unapproved cloud storage accounts that enabled users to upload information and share it with others both within and outside their organization. Although an authorized version was available that included stricter security controls, our review of a particular file sharing service identified 627 unmanaged accounts registered to Department Headquarters' email addresses, including 376

[7] NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, requires that individual security controls applicable to a system be identified and assessed in support of the system's authorization.

that were currently active. Unmanaged accounts are known as such because they are not affiliated with an enterprise license and, therefore, are not centrally managed to ensure information is protected according to the enterprise's requirements. The unmanaged accounts contained 464 gigabytes of stored information, and users were Department and contractor staff at various levels of the organization, including senior management, cybersecurity, and intelligence officials. The cloud service provider informed us that there were at least six more programs or sites across the Department that had large numbers of unmanaged accounts registered under their email addresses. Due to the inability to access specific content and documents, we could not determine whether sensitive information was stored in the unmanaged accounts.

Using cloud systems that are not organizationally managed potentially introduces significant risks to the Department's data. When unmanaged systems are used, the Department does not have visibility into user accounts, or the data stored in those accounts, and cannot ensure that required controls over uploading and sharing data are in place and operating effectively. In addition, the use of unmanaged cloud systems circumvents the Department's responsibility to identify and accept the risks associated with the system through the assessment and authorization process.

Cloud Systems Inventory

The Department did not have an accurate inventory of cloud-based systems used across the enterprise. For instance, we found that programs and sites generally used many more cloud computing systems than they reported to the Department's OCIO. Specifically, at the beginning of our review, the OCIO was aware of 103 cloud-based systems at the 5 locations reviewed. However, during our test work, we determined that the 5 locations operated a total of 227 cloud-based systems. Systems not included within the OCIO's visibility were related to functions such as file sharing, video conferencing, and project management. While we acknowledge that the Department's tracking and quarterly reporting of cloud inventories for the Federal Information Security Modernization Act of 2014 represent a point in time, the differences between the OCIO and location inventories appeared too significant to be attributed to a timing issue.

The Federal Information Security Modernization Act of 2014 requires agencies to maintain an inventory of all systems and related integrated systems. It also requires testing of controls for every information system on a periodic basis based on the system's impact level but not less than annually. Additionally, the President's recent Executive Order, *Improving the Nation's Cybersecurity*, requires agencies to implement Zero Trust Architecture. One of the primary steps in implementing Zero Trust Architecture is the creation of an inventory of systems, software, and other resources. Inaccuracies in the Department's system inventory could negatively impact efforts to transition to a Zero Trust Architecture. The Department also cannot accurately report information important to Federal decision-making if its locations continue to under-report their system inventories.

Contributing Factors

The issues identified occurred, in part, because the Department and its contractors had not fully implemented Federal requirements for managing cloud-based systems. In particular, the locations reviewed had not always implemented requirements for system authorizations, including security control assessments, and continuous monitoring. In addition, the Department had not issued overall guidance and requirements related to implementing cloud computing systems. Specifically, the Department had not issued enterprise-level policies and procedures related to preventing the use of unmanaged cloud systems, ensuring the Department's cloud systems inventory was complete and accurate, and identifying instances where the use of non-FedRAMP certified systems would be permitted.

Implementing Cloud System Requirements

The NIST Risk Management Framework outlines the requirements for assessing controls, authorizing systems for operation, and monitoring system controls once implemented. The Risk Management Framework applies to all types of Federal information systems, including cloud-based services and systems. Contrary to NIST direction, several locations did not always adhere to the Risk Management Framework requirements. In at least one case, this also led to overreliance on FedRAMP.

We determined that certain locations had not ensured that all cloud-based systems were appropriately authorized by Federal officials and that the process included the selection and assessment of security controls. Although Federal requirements allow tailoring of security controls in certain circumstances, they do not relieve officials of the responsibility of selecting and implementing security controls or authorizing the system. As noted in this report, two sites had not adhered to Federal requirements that mandated the identification and acceptance of risk by the Authorizing Official. Another site had not followed FedRAMP requirements for identification and assessment of controls outlined in cloud service providers' customer responsibility matrices. Further, a fourth site had not updated its security control assessments in over 5 years, resulting in the exclusion of numerous cloud-related controls. Given the variations in cloud system implementations at four of the five sites we reviewed, Department programs should ensure implementation of required authorization and assessment of security controls for cloud systems, including fully and appropriately using FedRAMP.

We also found that locations reviewed had not always modified continuous monitoring processes to utilize all available information to ensure cloud systems were operating within the site's risk tolerance, including keeping the Authorizing Official aware of any system changes. Three of the five sites included in our audit had not always reviewed continuous monitoring reports available through FedRAMP either because they assumed other organizations were monitoring the cloud systems, or they considered the process was too burdensome for contractors to access FedRAMP reports. Officials at one site demonstrated that they reviewed FedRAMP reports annually for a few selected systems; however, FedRAMP reports are available monthly. To realize the benefits of using FedRAMP certified systems, programs and field sites must incorporate available continuous monitoring reports into their existing risk management processes. At two of the three locations where we identified continuous monitoring issues, site officials explained that cloud systems were implemented and managed by a Department contractor and commented that contractors could not obtain permanent access to FedRAMP continuous monitoring reports. However, according to FedRAMP officials, contractors can be granted permanent access to reports when the cloud system is authorized by the agency and a Federal official requests permanent access for the contractor. Contractor officials agreed that continuous monitoring reports should have been obtained and reviewed with some frequency. However, none of the three locations had included this activity in their continuous monitoring policies and procedures.

Guidance on Implementing Cloud Systems

To its credit, the OCIO published the *DOE Cloud Smart Reference Guide* in 2020, which related to adoption and implementation strategies of cloud systems including best practices and guiding principles. However, as noted in Department Order 205.1C, *Department of Energy Cybersecurity Program*, these documents are non-binding, amplifying guidance. In addition, while the guide referenced either using FedRAMP systems or performing a significant approval process for a cloud system, it did not identify them as requirements for implementation of cloud systems. Our review of available policies and procedures found that the Department had not issued guidance to:

- Develop monitoring or other processes to identify and prevent the use of unmanaged cloud systems or services or to require that managed versions of FedRAMP-authorized systems be used. The specific cloud-based file sharing system in our review allowed managed account administrators to run monitoring reports to identify unmanaged accounts. However, locations that had a managed instance of the service might not have been using this report, which may have contributed to the large number of unmanaged accounts we identified. Notably, one site implemented an automated process to disallow unknown domains from accessing its file sharing cloud service.

- Ensure all cloud systems or services used by field sites were appropriately included in the Department's system inventory. We also determined that there was no process to verify that the systems and services reported to the Department's OCIO were complete and accurate. For example, none of the unauthorized systems at one location reviewed were included in the Department's inventory of cloud systems. According to the OCIO officials, a data call for cloud systems is issued quarterly. However, the officials also stated that many field sites did not report all cloud systems, with some sites not reporting any cloud-based systems. An accurate inventory is important to ensure that the Department is aware of where its information resides; however, that inventory cannot be accurately reported without additional guidance to provide detailed expectations.

- Define when non-FedRAMP cloud systems or services could be used. Despite being required to use FedRAMP for acquisition of all cloud systems since the program's inception in 2011, the Department and its contractors frequently had not used FedRAMP certified products. In some instances, it may be appropriate and necessary to deviate from FedRAMP authorized products; however, the Department had not defined such instances. Without uniform guidance from the Department, sites implemented their own cloud acquisition strategies. For example, some sites in our review indicated that obtaining a FedRAMP certification was burdensome for a cloud service provider or that a non-FedRAMP cloud system or service was necessary to collaborate with other organizations that used that particular cloud offering. Conversely, one site in our review advised that it would not consider implementation of a cloud system unless the cloud service provider already had a FedRAMP authorization or would be willing to undergo a

FedRAMP authorization before the cloud system was put into place. Widely adopted use of FedRAMP authorized products could positively impact the issues we identified related to cloud service security assessments and authorization, continuous monitoring, and the use of unmanaged cloud systems.

Impact to the Department

Without improvements, the Department may not be adequately protected from the risks posed by the use of systems outside its physical network boundaries, such as unauthorized access and data exfiltration. NIST requires that the operation of all Federal information systems or systems containing Federal information must be approved by a Federal official. Additionally, without ongoing monitoring of cloud provider-implemented controls, the Department does not have a full understanding of the risks facing the systems that contain its information. The Department also cannot monitor for potential malicious activity or insider threats associated with access to unmanaged or unknown cloud systems. The continued use of unmanaged or unknown cloud platforms outside of the Department's control could significantly impact its efforts to move toward a Zero Trust Architecture.

Recommendations

To ensure existing system authorization and monitoring requirements are met, we recommend that the Administrator, National Nuclear Security Administration (NNSA), and the Under Secretary for Science and Innovation, require programs and contractors to:

1. Ensure all cloud-based systems are appropriately authorized by Federal officials, including selection and assessment of all relevant security controls; and

2. Ensure all cloud-based systems are appropriately reported for inclusion in the Department's cloud inventory.

Further, we recommend that the Under Secretary for Science and Innovation require programs and contractors to:

3. Submit agency authorizations to the FedRAMP Project Management Office for cloud-based systems that are FedRAMP-authorized; and

4. Modify continuous monitoring plans, policies, and procedures to include monitoring results from FedRAMP, where applicable.

To improve the Department's security over cloud-based systems, we recommend that the Chief Information Officer, in conjunction with the Administrator, NNSA, and the Under Secretary for Science and Innovation, develop and issue guidance and requirements to assess, authorize, and monitor cloud-based systems to:

5. Implement monitoring or security controls to identify and prevent unmanaged cloud systems; and

6. Direct when it is appropriate to use cloud systems that have not been FedRAMP-authorized.

Management Comments

Management concurred with Recommendations 1 through 5, and nonconcurred with Recommendation 6. For Recommendation 1, NNSA officials indicated that they require cloud-based systems to be appropriately authorized by Federal officials through *NNSA Supplemental Directive 205.1, Baseline Cybersecurity Program*, and considered the recommendation closed. The Undersecretary for Science and Innovation commented that it will work with programs and national laboratories under its purview to ensure that all cloud-based systems are appropriately authorized by Federal officials, including selection and assessment of all relevant security controls.

For Recommendations 2 through 4, management concurred with the recommendations and described planned actions and estimated completion dates to ensure cloud-based systems are reported for inclusion in the Department's cloud inventory; agency authorizations are submitted to the FedRAMP Project Management Office for cloud-based systems that are FedRAMP authorized; and continuous monitoring plans, policies, and procedures are modified to include monitoring results from FedRAMP, where applicable.

The OCIO concurred with Recommendation 5 and indicated that it plans to issue updated guidance by the end of 2023 to address the tracking of all cloud systems. The OCIO nonconcurred with Recommendation 6. Management stated that the recently passed FedRAMP Authorization Act contains very specific language regarding the use of the program and the use of systems that are in the FedRAMP Marketplace. Management commented that if a system is not in the FedRAMP Marketplace, there are directions for an organization to meet specific security protocols during the assessment and authorization process of that cloud service system prior to being allowed onto the enterprise network. Additionally, management stated that the OCIO requires all organizations to be compliant with the FedRAMP Authorization Act and the policy contained in Department Order 205.1C. Consequently, management considered this recommendation closed.

Office of Inspector General Response

Management's comments and planned corrective actions were responsive for Recommendations 1 through 5. Based on corrective actions already taken, we consider Recommendation 1 closed for NNSA. However, Recommendation 1 remains open for the Under Secretary for Science and Innovation. Further, based on the recently passed FedRAMP Authorization Act and additional information provided by the OCIO, we consider Recommendation 6 closed.

Appendix 1

Commonly Used Terms

Department of Energy	Department
Federal Risk and Authorization Management Program	FedRAMP
National Institute of Standards and Technology	NIST
National Nuclear Security Administration	NNSA
Office of the Chief Information Officer	OCIO
Special Publication	SP

Objective, Scope, and Methodology

Objective

The objective of this audit was to determine whether the Department of Energy effectively implemented security over its cloud-based technologies and services.

Scope

The audit was remotely performed from January 2021 through December 2022 with officials working at Department Headquarters in Washington, DC, and Germantown, Maryland; Idaho National Laboratory in Idaho Falls, Idaho; Ames National Laboratory in Ames, Iowa; and Nevada National Security Site in North Las Vegas, Nevada. The scope was limited to current cloud systems and cloud implementation practices. The audit was conducted under Office of Inspector General project number A21TG006.

Methodology

To accomplish our objective, we:

- Reviewed Federal and Department policies and procedures, directives, laws, and regulations specific to the audit;

- Reviewed prior reports issued by the Office of Inspector General, the Government Accountability Office, and the Department's Office of Enterprise Assessments as they related to our audit objective;

- Held discussions with officials from the Office of the Chief Information Officer, Office of Science, Ames Site Office, Ames National Laboratory, Idaho Operations Office, Idaho National Laboratory, Nevada Field Office, and the Nevada National Security Site;

- Reviewed documentation related to cloud systems controls assessments and authorizations at sites selected for review; and

- Coordinated with a cloud service provider to identify unmanaged users and other information from that system.

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 and appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Accordingly, we assessed internal controls and compliance with laws and regulations necessary to satisfy the audit objective. In particular, we assessed the following internal control components and underlying principles significant to the audit objective: control environment and the related principle to demonstrate commitment to competence; risk assessment and the principle related to identify, analyze, and respond to risk; control activities and the principles related to design activities for information systems, design control activities, and implement control activities; information and communication and the related principles to communicate externally and communicate internally; and monitoring and the related principles to perform monitoring activities and remediate deficiencies. However, because our review was limited to 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. We relied on computer-processed data to satisfy our objective and tested the validity of the data by verifying that data to source documents. While we identified weaknesses related to the implementation of cloud services in the Department, we determined overall that the data was sufficiently reliable for the purposes of our audit objective.

Management waived an exit conference on March 14, 2023.

Related Reports

Office of Inspector General

- Audit Report on the *Department of Energy's Management of Legacy Information Technology Infrastructure* (DOE-OIG-19-22, March 2019). We determined that while actions to manage the lifecycle of unsupported information technology (IT) systems and components had been taken at the sites reviewed, opportunities for improvement existed. For example, the Department of Energy, including contractor-managed locations, had not developed a comprehensive plan to identify and replace legacy IT. Our review of several sites did not reveal any requirements within the Department to identify and eliminate legacy IT. As such, we made one recommendation that, if fully implemented, should improve the Department's management of legacy IT.

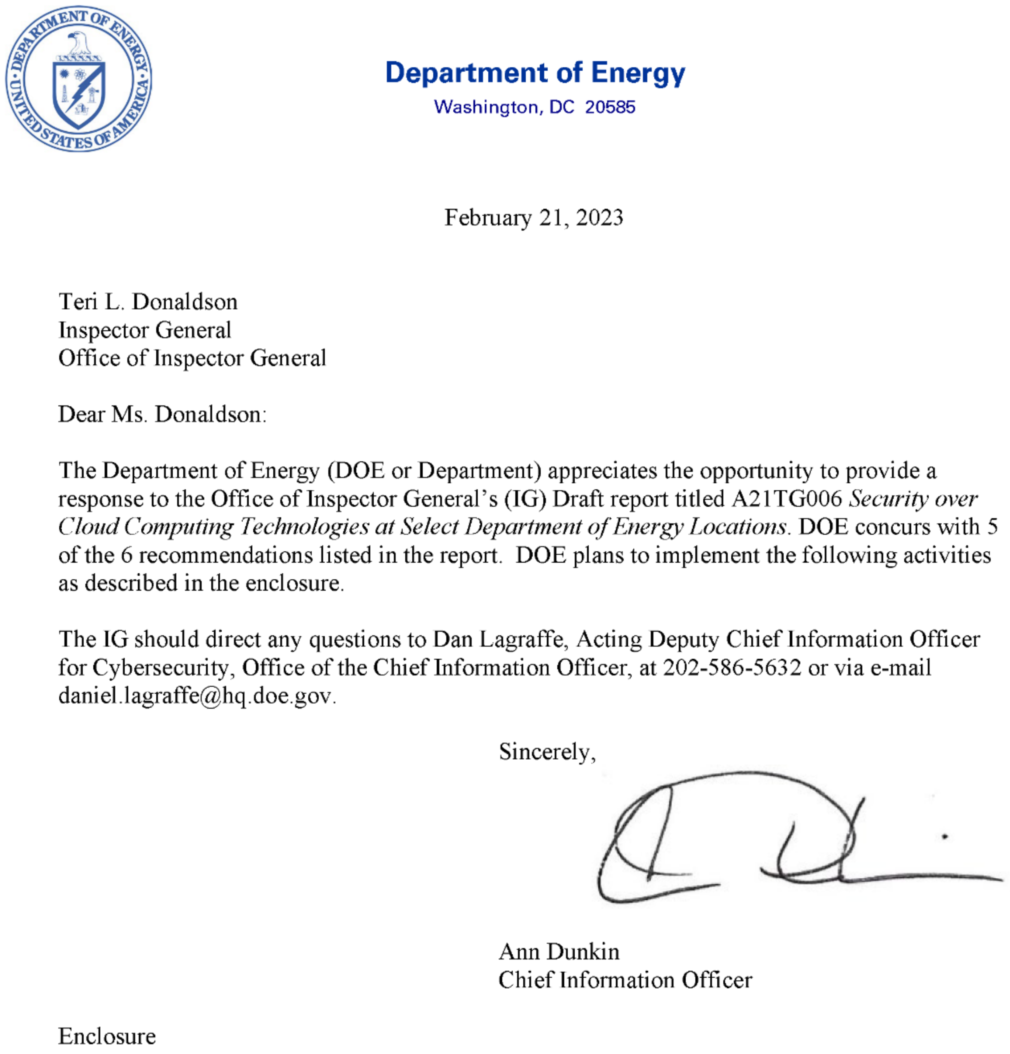
- Audit Report on *The Department of Energy's Management of Cloud Computing Activities* (DOE/IG-0918, September 2014). The Department had not always effectively or efficiently acquired, implemented, or managed its cloud computing technologies. In particular, we found: (1) programs and sites independently acquired and managed cloud computing services valued at more than $30 million; however, the Department had not developed and maintained a complete inventory of cloud services to help manage its efforts; (2) the Department had not always established contracts with cloud computing service providers that ensured effective controls over the management of stored or transmitted information; and (3) the Department had not ensured that cloud computing services were implemented in accordance with the Federal Risk and Authorization Management Program. These issues occurred, in part, because the Department lacked a comprehensive strategy designed to ensure effective and efficient implementation of cloud computing technologies. 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. 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.

Government Accountability Office

- *CLOUD COMPUTING SECURITY: Agencies Increased Their Use of the Federal Authorization Program, but Improved Oversight and Implementation Are Needed* (GAO-20-126, December 2019).

Appendix 4

Management Comments



Department of Energy
Washington, DC 20585

February 21, 2023

Teri L. Donaldson
Inspector General
Office of Inspector General

Dear Ms. Donaldson:

The Department of Energy (DOE or Department) appreciates the opportunity to provide a response to the Office of Inspector General's (IG) Draft report titled A21TG006 *Security over Cloud Computing Technologies at Select Department of Energy Locations*. DOE concurs with 5 of the 6 recommendations listed in the report. DOE plans to implement the following activities as described in the enclosure.

The IG should direct any questions to Dan Lagraffe, Acting Deputy Chief Information Officer for Cybersecurity, Office of the Chief Information Officer, at 202-586-5632 or via e-mail daniel.lagraffe@hq.doe.gov.

Sincerely,

Ann Dunkin
Chief Information Officer

Enclosure

MANAGEMENT Response
OIG Draft Report, A21TG006
Security over Cloud Computing Technologies at Select Department of Energy Locations

To ensure existing system authorization and monitoring requirements are met, we recommend that the Administrator, National Nuclear Security Administration, and the Under Secretary for Science and Innovation, require programs and contractors to:

Recommendation 1. Ensure all cloud-based systems are appropriately authorized by Federal officials, including selection and assessment of all relevant security controls; and

Management Response: NNSA Concurs in Principle

NNSA requires cloud-based systems to be appropriately authorized by Federal officials through NNSA Supplemental Directive (SD) 205.1, *Baseline Cybersecurity Program.* Authority to Operate (ATO) packages may leverage previously assessed cloud services as long as they are reviewed and approved according to the Federal Risk and Authorization Management Program (FedRAMP) process described in the FedRAMP Concept of Operations (CONOPS). Cloud service providers that have not been FedRAMP-certified are required to follow the FedRAMP security assessment process per the FedRAMP CONOPS, which requires the assessment of all relevant security controls. Regarding the auditors' observations at an NNSA site, the concerns were identified and appropriate corrective actions were initiated prior to the IG audit, as acknowledged in the audit report.

Estimated Completion Date: NNSA considers this recommendation closed.

Management Response: Office of the Undersecretary for Science and Innovation Concurs

The Office of the Undersecretary for Science and Innovation will work with all S4 programs and corresponding National Labs to ensure all cloud-based systems are appropriately authorized by Federal officials, including selection and assessment of all relevant security controls.

Estimated Completion Date: 12/31/2023

Recommendation 2: Ensure all cloud-based systems are appropriately reported for inclusion in the Department's cloud inventory.

Management Response: NNSA Concurs

NNSA SD 205.1, *Baseline Cybersecurity Program,* currently requires all NNSA locations to report their cloud-based systems in accordance with the Department's guidelines. Per the SD, NNSA requires sites to list their cloud-based systems into the Enterprise Governance, Risk, and Compliance (eGRC) tool. NNSA assesses the systems listed in the eGRC tool against those they report on a quarterly basis through the Federal Information Security Modernization Act (FISMA), which requires agencies to provide metrics to the Office of Management and Budget. FISMA's metrics include a report that identifies the types of Cloud Services the Agency is using and what service(s) they are receiving. (e.g., mail, database, applications, etc.). To validate the number of cloud-based systems being reported, NNSA will compare the FISMA metrics reported in the first quarter of FY 2023 to the cloud-based systems reported in eGRC.

Estimated Completion Date: 03/31/2023

Management Response: Office of the Undersecretary for Science and Innovation Concurs

The Office of the Undersecretary for Science and Innovation will work with all S4 programs and corresponding National Labs to ensure all cloud-based systems are appropriately reported for inclusion in the Department's cloud inventory.

Estimated Completion Date: 12/31/2023

Further, we recommend that the Under Secretary for Science and Innovation require programs and contractors to:

Recommendation 3: Submit agency authorizations to the FedRAMP Project Management Office for cloud-based systems that are FedRAMP-authorized; and

Management Response: Concur

The Office of the Undersecretary for Science and Innovation will work with all S4 programs and corresponding National Labs to ensure agency authorizations to the FedRAMP Project Management Office for cloud-based systems that are FedRAMP-authorized are submitted in a timely manner by 2024.

Estimated Completion Date: 12/31/2023

Recommendation 4: Modify continuous monitoring plans, policies, and procedures to include monitoring results from FedRAMP, where applicable.

Management Response: Concur

The Office of the Undersecretary for Science and Innovation will work with all S4 programs and corresponding National Labs to ensure monitoring plans, policies, and procedures are continuously updated and will provide documentation on plans and include monitoring results from FedRAMP.

Estimated Completion Date: 12/31/2023

To improve the Department's security over cloud-based systems, we recommend that the Chief Information Officer, in conjunction with the Administrator, National Nuclear Security Administration, and the Under Secretary for Science and Innovation, develop and issue guidance and requirements to assess, authorize, and monitor cloud-based systems to:

Recommendation 5: Implement monitoring or security controls to identify and prevent unmanaged cloud systems; and

Management Response: Concur

In order to monitor all DOE information systems, including all cloud systems, the DOE OCIO utilizes our Enterprise Cyber Governance System (ECGS) for FISMA inventory and reporting. OCIO also leverages Directive 205.1C, Department of Energy Cybersecurity Program which requires all DOE Departmental Elements (DE) to have Cyber Security Program Plans (CSPP).

- Per DOE D 205.1C Cybersecurity Program:
    - "To implement the DOE Cybersecurity Program, the Department maintains:
        - CSPPs, which are required for all DOE DEs and their associated sites that manage IT/OT systems. DE-CSPPs and Site CSPPs must cover all DOE systems and all DOE IT assets."

- The DOE OCIO Enterprise Cybersecurity Program Plan (E-CSPP) states:
    - "System Inventory
        - DOE O 205.1C mandates that Departmental Elements will address requirements for their system inventory in their CSPPs and update the DOE Cybersecurity Data Repository within the ECGS with their FISMA systems and status on a quarterly basis.
        - Each Departmental Element is responsible for the accounting of each IT and computing asset under their purview…
        - The FISMA Inventory Methodology will address requirements for identification of enhanced control types including HVAs, PII and other CUI-specified information types, as well as the use of cloud services and the Federal Risk and Authorization Management Program (FedRAMP) process."

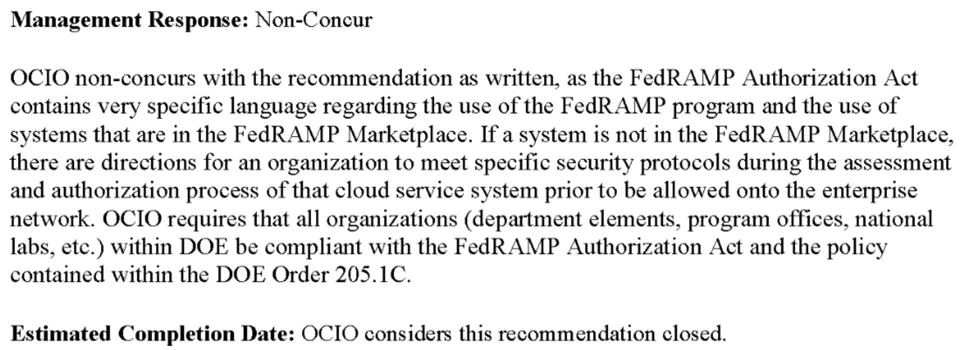
Additionally, in November 2022, OCIO published its "Improving Cybersecurity: Headquarters Cloud Technology Adoption Plan" and maturity assessment tool as amplification guidance for use by the departmental elements (DEs) to promulgate mission-specific guidance to their offices, laboratories, and sites. Each DE that does not fall directly under the headquarters plan is responsible for developing a Cloud Plan program that ensures cloud adoption is managed and assessed in accordance with Executive Order 14028 requirements. To date, we have received more than 93% of the required individual departmental plans and are currently reviewing them to provide critical feedback. Plans received include coverage for Idaho National Laboratory and Ames Laboratory. The Nevada National Security Site's compliance is being tracked by NNSA.

As we continually review our processes and procedures, the next iteration of 205 (1D) will be enhanced to address the tracking of 'all' cloud systems. The anticipated publishing date of DOE Directive 205.1D is by the end of the 2023 calendar year.

Estimated Completion Date: 12/31/2023

Recommendation 6: Direct when it is appropriate to use cloud systems that have not been FedRAMP authorized.

Appendix 4



Management Response: Non-Concur

OCIO non-concurs with the recommendation as written, as the FedRAMP Authorization Act contains very specific language regarding the use of the FedRAMP program and the use of systems that are in the FedRAMP Marketplace. If a system is not in the FedRAMP Marketplace, there are directions for an organization to meet specific security protocols during the assessment and authorization process of that cloud service system prior to be allowed onto the enterprise network. OCIO requires that all organizations (department elements, program offices, national labs, etc.) within DOE be compliant with the FedRAMP Authorization Act and the policy contained within the DOE Order 205.1C.

Estimated Completion Date: OCIO considers this recommendation closed.

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 OIG.Reports@hq.doe.gov and include your name, contact information, and the report number. You may also mail comments to us:

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 202–586–1818. For media-related inquiries, please call 202–586–7406.