May 2023

CLOUD SECURITY

Selected Agencies Need to Fully Implement Key Practices

CLOUD SECURITY

Selected Agencies Need to Fully Implement Key Practices

Why GAO Did This Study

Cloud computing provides agencies with potential opportunities to obtain IT services more efficiently; however, if not effectively implemented, it also poses cybersecurity risks. To facilitate the adoption and use of cloud services, the Office of Management and Budget and other federal agencies have issued policies and guidance on key practices that agencies are to implement to ensure the security of agency systems that leverage cloud services (i.e., cloud systems).

This report evaluates the extent to which selected agencies have effectively implemented key cloud security practices. To do so, GAO selected 15 cloud systems across four agencies (Agriculture, DHS, Labor, and Treasury), representing a broad range of services. GAO selected these agencies based on several factors, including the number of reported IT investments leveraging cloud computing. GAO compared relevant agency documentation against six key practices identified in federal policies and guidance. GAO rated each agency as having fully, partially, or not implemented each practice for the selected systems.

What GAO Recommends

GAO is making 35 recommendations to four agencies to fully implement key cloud security practices. DHS concurred with the recommendations. Agriculture, Labor, and Treasury neither agreed nor disagreed with the recommendations. DHS, Labor, and Treasury described actions taken or planned to address the recommendations.

View GAO-23-105482. For more information, contact David B. Hinchman at (214) 777-5719 or hinchmand@gao.gov, or Brian Bothwell at (202) 512-6888 or bothwellb@gao.gov.

What GAO Found

The four selected agencies—the Departments of Agriculture, Homeland Security (DHS), Labor, and the Treasury—varied in their efforts to implement the six key cloud security practices that GAO evaluated. Specifically, three agencies fully implemented three practices for most or all of their selected systems, while another agency fully implemented four practices for most or all of its systems. However, the agencies partially implemented or did not implement the other practices for the remaining systems (see figure).

Agencies' Implementation of the Key Cloud Security Practices for Each of the Selected Systems
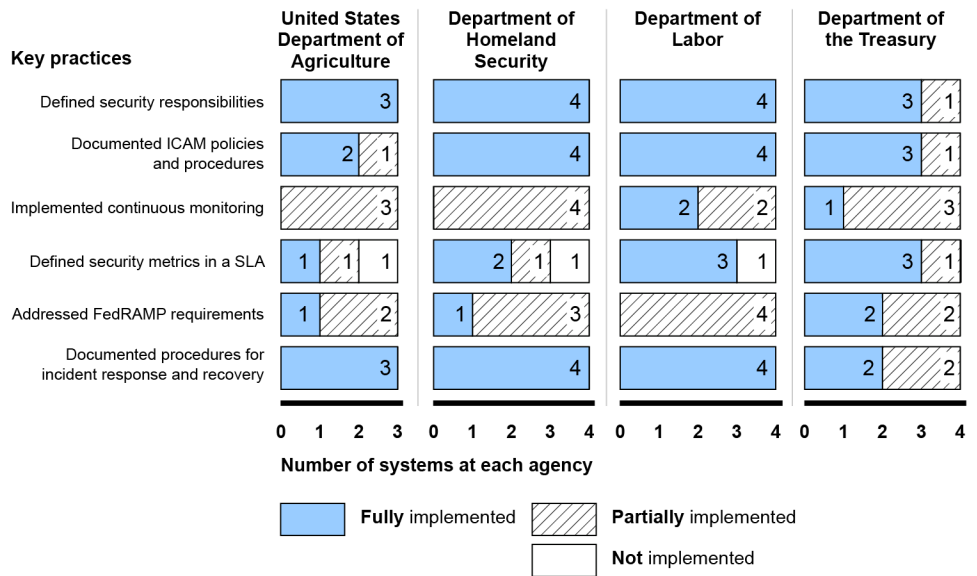
ICAM (Identity, Credential, and Access Management), SLA (service level agreement), FedRAMP (Federal Risk and Authorization Management Program)

Source: GAO analysis of agency data. | GAO-23-105482

For example, the agencies partially implemented the practice regarding continuous monitoring for some or all of the systems. Although the agencies developed a plan for continuous monitoring, they did not always implement their plans. In addition, agencies partially implemented or did not implement the practice regarding service level agreements for some of the systems. Specifically, agencies' service level agreements did not consistently define performance metrics, including how they would be measured, and the enforcement mechanisms.

Agency officials cited several reasons for their varied implementation of the key practices, including acknowledging that they had not documented their efforts to address the requirements. Until these agencies fully implement the cloud security key practices identified in federal policies and guidance, the confidentiality, integrity, and availability of agency information contained in these cloud systems is at increased risk.

_____ **United States Government Accountability Office**

Contents

Figures

GAO

U.S. GOVERNMENT ACCOUNTABILITY OFFICE

441 G St. N.W.
Washington, DC 20548

May 18, 2023

The Honorable Frank Lucas
Chairman
The Honorable Zoe Lofgren
Ranking Member
Committee on Science, Space, and Technology
House of Representatives

The Honorable Jamie Raskin
Ranking Member
Committee on Oversight and Accountability
House of Representatives

The Honorable Gerald E. Connolly
Ranking Member
Subcommittee on Cybersecurity, Information Technology, and
Government Innovation
Committee on Oversight and Accountability
House of Representatives

As part of a comprehensive effort to transform IT within the federal government, in 2010 the Office of Management and Budget (OMB) began requiring agencies to shift their IT services to a cloud computing option when feasible.[1] According to the National Institute of Standards and Technology (NIST), cloud computing is a means for enabling on-demand access to shared pools of configurable computing resources (e.g., networks, servers, storage applications, and services) that can be rapidly provisioned and released. Cloud services offers federal agencies a means to buy services more quickly and possibly at a lower cost than building, operating, and maintaining these computing resources themselves.

However, as we have previously reported, the use of cloud computing also poses cybersecurity risks.[2] These risks arise when agencies and cloud service providers (CSP) do not effectively implement security

---

[1]Office of Management and Budget, *25 Point Implementation Plan to Reform Federal Information Technology Management* (Dec. 9, 2010).

[2]GAO, *Information Security: Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing*, GAO-10-513 (Washington, D.C.: May 27, 2010).

GAO-23-105482 Federal Cloud Environment

controls over cloud services. Weaknesses in these controls could lead to vulnerabilities affecting the confidentiality, integrity, and availability of agency information.

To facilitate the adoption and use of cloud services, OMB has issued policies on key practices that agencies are to implement to ensure the security of agency systems that leverage cloud services (i.e., cloud systems). Further, federal agencies, including the Department of Homeland Security (DHS), General Services Administration (GSA), and NIST have developed guidance to assist agencies in implementing these policies, including key practices for securing cloud systems.

We performed our work under the authority of the Comptroller General to conduct evaluations on agencies' implementation of key cloud security practices to assist Congress with its oversight responsibilities. Specifically, this report evaluates the extent to which selected agencies have effectively implemented key cloud security practices.

To address this objective, we identified a nongeneralizable sample of four Chief Financial Officers Act agencies[3] that were using cloud services. Specifically, we selected the Departments of Agriculture, Homeland Security, Labor, and the Treasury. We selected these agencies based on several factors, including the number of reported IT investments leveraging cloud computing in fiscal year 2021, in order to find a mix of agencies with a heavy and moderate use of cloud services.

We then selected a sample of cloud systems from each of the agencies that represented a broad range of services.[4] Specifically, we selected four systems for three of the four agencies (DHS, Labor, and Treasury), and

---

[3]The 24 agencies covered by the *Chief Financial Officers Act of 1990* are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Personnel Management; Small Business Administration; Social Security Administration; and the U.S. Agency for International Development (31 U.S.C. § 901(b)).

[4]Federal agencies can select different cloud services to support their missions. These services can range from a basic computing infrastructure on which agencies run their own software, to a full computing infrastructure that includes software applications. The types of cloud services are discussed in a subsequent section of this report.

three cloud systems from one agency (Agriculture).[5] Due to sensitivity concerns, we are not disclosing the names of the systems in this report.

To identify key cloud security practices, we analyzed federal IT policies (e.g., federal cloud strategy) and federal guidance (e.g., the Cloud Security Technical Reference Architecture).[6] To help in identifying the relevant guidance, in January 2022 and April 2022, we held expert panels with public and private sector experts, respectively, to discuss these and other cloud security guidance. Appendix I lists the participants and their corresponding organizations from both panels.

From our review of the relevant guidance, we selected six key cloud security practices that agencies should apply to their cloud systems, as well as associated evaluation criteria for each practice. All six key cloud security practices, and the associated evaluation criteria, are detailed in a subsequent section of this report.

We then obtained documentation from each agency, including system security plans, contracts, incident response plans, and contingency plans. We analyzed these documents to determine whether the agency had implemented the six key practices for each of the agency's selected cloud systems. For each system, we first assessed the agency's implementation of our evaluation criteria within each practice as:

- fully implemented—the agency provided evidence which showed that it fully or largely addressed the elements of the criteria.

- partially implemented—the agency provided evidence that showed it had addressed at least part of the criteria.

- not implemented—the agency did not provide evidence that it had addressed any part of the criteria.

---

[5]We initially selected four systems from Agriculture; however, during our review, Agriculture transferred responsibility for one selected system to GSA. Since Agriculture no longer had security responsibilities for the system, we removed the system from our review. Based on our engagement timelines, we decided to not select a new system for our evaluation. As a result, our review for Agriculture only included three cloud systems.

[6]Among others, Office of Management and Budget, *Federal Cloud Computing Strategy* (Washington, D.C.: June 2019); and Cybersecurity and Infrastructure Security Agency, U.S. Digital Service, and FedRAMP, *Cloud Security Technical Reference Architecture* (Washington, D.C.: Aug. 2021).

To determine an overall rating for each of the six key cloud security practices for an individual system, we then summarized the results of our assessments of the evaluation criteria by assessing each key practice as:

- fully implemented—the agency provided evidence that showed that it fully implemented each evaluation criteria.

- partially implemented—the agency provided evidence that showed it had partially or fully implemented at least one or more of the evaluation criteria, but did not fully implement each criteria.

- not implemented—the agency did not provide evidence that it had implemented any part of the evaluation criteria.

We supplemented our analysis with interviews of relevant agency officials about their efforts to implement the key cloud security practices. Appendix II includes additional information on our objective, scope, and methodology.

We conducted this performance audit from October 2021 to May 2023 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

As federal agencies increasingly use cloud computing to perform their missions, the implementation of effective security practices becomes more important. OMB has issued policies directing agencies to implement practices for securing their cloud systems. For example:

- In December 2011, OMB's memorandum on the *Security Authorization of Information Systems in Cloud Computing Environments* sets policy for federal agencies to protect information in the cloud through adoption of the Federal Risk and Authorization Management Program (FedRAMP).[7] The memorandum called for agencies to use FedRAMP when conducting risk assessments, security authorizations, and granting authority to operate (ATO). Further, the memorandum called for agencies to ensure that the agency's contract required the CSP to comply with FedRAMP security

[7]Office of Management and Budget, *Security Authorization of Information Systems in Cloud Computing Environments* (Washington, D.C.: Dec. 8, 2011).

authorization requirements. In addition, the memorandum called for agencies to establish and implement a response plan for security and privacy incidents for the cloud service, among other things.[8]

- In June 2019, OMB issued the *Federal Cloud Computing Strategy* that includes requirements and guidance for federal agencies to implement cloud computing.[9] For example, the strategy included guidance related to implementing an Identity, Credential, and Access Management (ICAM) process and performing continuous monitoring of agencies' cloud systems.[10]

- In August 2021, OMB released its memorandum on *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, which established requirements for logging, log retention, and log management, among other things.[11]

- In January 2022, OMB released its memorandum on *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, which required agencies to meet specific cybersecurity standards and objectives by the end of fiscal year 2024.[12] For example, the memorandum provided guidance on implementing identity and access controls, including the use of multifactor authentication, among other things.

In addition, federal agencies, including NIST, GSA, and DHS's Cybersecurity and Infrastructure Security Agency (CISA), have issued

---

[8]The recently enacted *FedRAMP Authorization Act* codified the FedRAMP program. According to the act, GSA is responsible for establishing a government-wide program that provides a standardized, reusable approach to security assessment and authorization for cloud computing products and services that process unclassified information used by agencies. James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. No. 117-263, div. E, title LIX, subtitle C, § 5921(a), 136 Stat. 3449, 3450 (December 23, 2022), codified at 44 U.S.C. §3608.

[9]Office of Management and Budget, *Federal Cloud Computing Strategy* (Washington, D.C.: June 24, 2019).

[10]ICAM refers to the set of tools, policies, and systems that an agency uses to enable the right individual to access the right resource, at the right time, and for the right reason, in support of federal business objectives.

[11]Office of Management and Budget, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, OMB Memorandum M-21-31 (Washington, D.C.: Aug. 27, 2021).

[12]Office of Management and Budget, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, OMB Memorandum M-22-09 (Washington, D.C.: Jan. 26, 2022).

related guidance that further define key practices for securing cloud systems. For example,

- In December 2011, NIST issued guidance on cloud security challenges.[13] In addition, in July 2020, NIST issued guidance on access controls for cloud systems, including on developing policies and procedures.[14]

- In November 2017, the FedRAMP Program Management Office (PMO), which is part of GSA, established a framework for authorizing cloud services and to assist agencies with meeting the FedRAMP requirements for cloud services they use.[15] For example, according to the framework, agencies should ensure that contracts with CSPs require them to comply with FedRAMP requirements. Further, the agency should provide a copy of its authorization letter for the cloud service (cloud service authorization letter) to the FedRAMP PMO. In addition to the framework, the PMO issued guidance on how agencies can leverage[16] existing security authorization packages.[17] GSA has issued additional guidance on acquiring cloud services, including on the importance of having a service level agreement (SLA) with the CSP.[18]

- In August 2021, CISA issued guidance to provide recommended approaches to cloud migration and data protection.[19] For example, the guidance provided information on practices for monitoring agencies'

---

[13]National Institute of Standards and Technology, *Guidelines on Security and Privacy in Public Cloud Computing*, SP 800-144 (Gaithersburg, MD: Dec. 2011).

[14]National Institute of Standards and Technology, *General Access Control Guidance for Cloud Systems*, SP 800-210 (Gaithersburg, MD: July 2020).

[15]FedRAMP Program Management Office, *FedRAMP Security Assessment Framework* (Washington, D.C.: Nov. 15, 2017).

[16]According to OMB, leveraged authorizations can be used when an agency chooses to accept some or all of the information in an existing authorization package generated by another agency based on the need to use the same information resources (e.g., information system or services provided by the system).

[17]FedRAMP, *Agency Guide For FedRAMP Authorizations: How to Functionally Reuse an Existing Authorization Version 2.0* (Washington, D.C.: Dec. 7, 2017).

[18]General Services Administration, *Federal Cloud Strategy Guide Agency Best Practices for Cloud Migration* (Washington, D.C.: Feb. 2021); and *Cloud Adoption Center of Excellence Playbook* (Washington, D.C.: Sept. 2020).

[19]Cybersecurity and Infrastructure Security Agency, U.S. Digital Service, and FedRAMP, *Cloud Security Technical Reference Architecture* (Washington, D.C.: Aug. 2021).

cloud systems, such as on the use of vulnerability management procedures and tools to monitor the agency's cloud infrastructure, and on collecting and reviewing audit logs to detect anomalies in activity. Further, the guidance stated that agencies should document procedures for responding to and recovering from security and privacy incidents for the cloud system.

Agencies Can Select from a Number of Cloud Service and Deployment Models

Federal agencies can select different cloud services to support their missions. These services can range from a basic computing infrastructure on which agencies run their own software, to a full computing infrastructure that includes software applications. In defining cloud service models, NIST identifies three primary service models:

- Infrastructure as a Service (IaaS). The CSP delivers and manages the basic computing infrastructure of servers, software, storage, and network equipment. The agency provides the operating system, programming tools and services, and applications.

- **Platform as a Service (PaaS)**. The CSP delivers and manages the infrastructure, operating system, and programming tools and services, which the agency can use to create applications.

- **Software as a Service (SaaS)**. The CSP delivers one or more applications and all the resources (operating system and programming tools) and underlying infrastructure, which the agency can use on demand.

Each type of cloud service offers unique features and carries its own security implications that agencies should consider when implementing their cloud systems. For example, as shown in figure 1, agencies have most of the security responsibilities for IaaS, whereas CSPs have most of the responsibilities for SaaS.

Figure 1: Cloud Service Provider and Agency Responsibilities for Different Service Models

Infrastructure-as-a-Service	Platform-as-a-Service	Software-as-a-Service
Configuration	Configuration	Configuration
Identity and Access Management	Identity and Access Management	Identity and Access Management
Data	Data	Data
Networking	Networking	Networking
Application(s)	Application(s)	Application(s)
Runtime	Runtime	Runtime
Middleware	Middleware	Middleware
Operating System	Operating System	Operating System
Virtualization	Virtualization	Virtualization
Servers	Servers	Servers
Storage	Storage	Storage
Physical Security	Physical Security	Physical Security

Legend:
- Agency managed
- Managed by both
- Cloud service provider managed

Note: Identity and Access Management ensures that the right people and things have the right access to the right resources at the right time; Runtime is the period during which a computer program is executing; Middleware refers to software that connects computers and devices to other applications; Virtualization refers to the use of software instead of hardware to manage configurable network resources.

In addition, agencies can choose from a variety of arrangements for obtaining cloud services (called cloud deployment models), ranging from a private cloud for one organization to sharing a public cloud. NIST identified the following four cloud deployment models:

- **Private cloud**. The service is set up specifically for one organization, although there may be multiple customers within that organization and the cloud may exist on or off the organization's premises.

- **Community cloud**. The service is set up for organizations with similar requirements. The cloud may be managed by the organizations or a third party and may exist on or off the organizations' premises.

- **Public cloud**. The service is available to the general public and is owned and operated by the service provider.

- **Hybrid cloud**. The service is a composite of two or more of the three deployment models (private, community, or public) that are bound together by technology that enables data and application portability.

GAO Has Reported on Agencies' Efforts to Secure Cloud Systems

We have previously reported on agencies' efforts to secure cloud systems. For example:

- In December 2019, we reported that four selected agencies—the Department of Health and Human Services, GSA, the Environmental Protection Agency, and the U.S. Agency for International Development—did not consistently address key elements of the FedRAMP authorization process.[20] Specifically, these four agencies did not consistently or fully address required information in system security plans, security assessment reports, and remedial action plans. In addition, the agencies did not always prepare their authorizations approving the use of cloud services.

  We recommended, among other things, that the agencies address these key elements. GSA and the Department of Health and Human Services agreed with the recommendations, the U.S. Agency for International Development generally agreed, the Environmental Protection Agency generally disagreed, and OMB neither agreed nor disagreed. Since then, GSA and the U.S. Agency for International Development have implemented each of their related recommendations. The Department of Health and Human Services has implemented five of the 11 recommendations, but has not

---

[20]GAO, *Cloud Computing Security: Agencies Increased Their Use of the Federal Authorization Program, but Improved Oversight and Implementation Are Needed,* GAO-20-126 (Washington, D.C.: Dec. 12, 2019).

implemented the other six recommendations. The Environmental Protection Agency has not addressed any of the five recommendations.

- In April 2016, we reported that five agencies[21] had incorporated a majority of 10 key SLA practices in their cloud contracts.[22] These practices included identifying the roles and responsibilities of major stakeholders, defining performance objectives, and specifying security metrics. We recommended that the agencies implement SLA guidance and incorporate applicable key practices into their SLAs. Four agencies—the Departments of Defense, Health and Human Services, Homeland Security, and Veterans Affairs—agreed with our recommendations, and one agency (Treasury) had no comments. Since then, three of the agencies—the Departments of Defense, Homeland Security, and Veterans Affairs—had implemented our recommendations. The remaining two agencies—the Departments of Health and Human Services and the Treasury—had not fully addressed our recommendations.

Selected Agencies Varied in Their Implementation of Key Cloud Security Practices

As discussed previously, guidance issued by federal agencies, including OMB, GSA, DHS, and NIST, establishes cloud security practices for federal agencies. From this guidance, we selected six key practices for securing cloud systems. In addition, we identified evaluation criteria based on the related guidance for each of the key practices. Table 1 shows the six key practices and the associated evaluation criteria.

---

[21]The agencies included in the review were the Departments of Defense, Homeland Security, Health and Human Services, the Treasury, and Veterans Affairs.

[22]GAO, *Cloud Computing: Agencies Need to Incorporate Key Practices to Ensure Effective Performance,* GAO-16-325 (Washington, D.C.: Apr. 7, 2016).

Table 1: Selected Key Cloud Security Practices and Associated Evaluation Criteria

Key practice	Evaluation criteria
Define the delineation of security responsibilities between the agency and the cloud service provider (CSP) for the cloud system.	• The agency identified its control implementation responsibilities as well as that of the CSPs.
Document the identity, credential, and access management (ICAM) policies and procedures for the cloud system.	• The agency documented identity and authentication procedures for the cloud system, including the use of multifactor authentication for organizational users of the cloud system. • The agency documented access control policy and procedures that: (1) identified the authorized users of the system, group and role membership, and access authorizations; (2) identified, documented, and defined system access authorizations to support separation of duties; and (3) employed least privilege for specific duties and systems.
Develop and implement a plan for continuously monitoring the cloud system.	• The agency developed and implemented a plan for continuously monitoring the security controls that are the agency's responsibility. • The agency reviewed continuous monitoring deliverables from the CSP. • The agency documented the use of vulnerability management procedures and tools to monitor the agency's cloud infrastructure. • The agency collected and reviewed audit logs.
Define security metrics in a service level agreement (SLA) with the CSP.	• The agency's SLA with the CSP defined performance metrics. • The agency's SLA with the CSP defined how the performance would be measured. • The agency's SLA with the CSP defined the enforcement mechanisms to ensure the specified performance levels are achieved.
Use FedRAMP when conducting risk assessments, security authorizations, and granting an authority to operate for the cloud system.	• The agency leveraged a CSP that had a FedRAMP authorization. • The agency documented the authorization of (1) the agency system supported by the cloud service and (2) the cloud service used by the agency. • The agency provided a copy of its authorization letter for the cloud service (cloud service authorization letter) to the FedRAMP Program Management Office. • The agency's contract required the CSP to comply with FedRAMP security authorization requirements.
Document procedures for responding to and recovering from security and privacy incidents for the cloud system.	• The agency documented procedures for responding to and recovering from security and privacy incidents for the cloud system.

FedRAMP = Federal Risk and Authorization Management Program

Source: GAO analysis of federal policies and guidance. | GAO-23-105482

The four selected agencies varied in their efforts in implementing key cloud security practices for each of their selected systems. For example, the agencies fully documented security responsibilities for all but one of 15 selected systems. However, the agencies fully addressed FedRAMP requirements for four of the selected systems and partially implemented the requirements for the other 11 systems. Figure 2 provides the extent to

which agencies implemented the key practices for their selected systems. Each of the practices is discussed in more detail below.

Figure 2: Agencies' Implementation of the Key Practices for Each of the Selected Systems
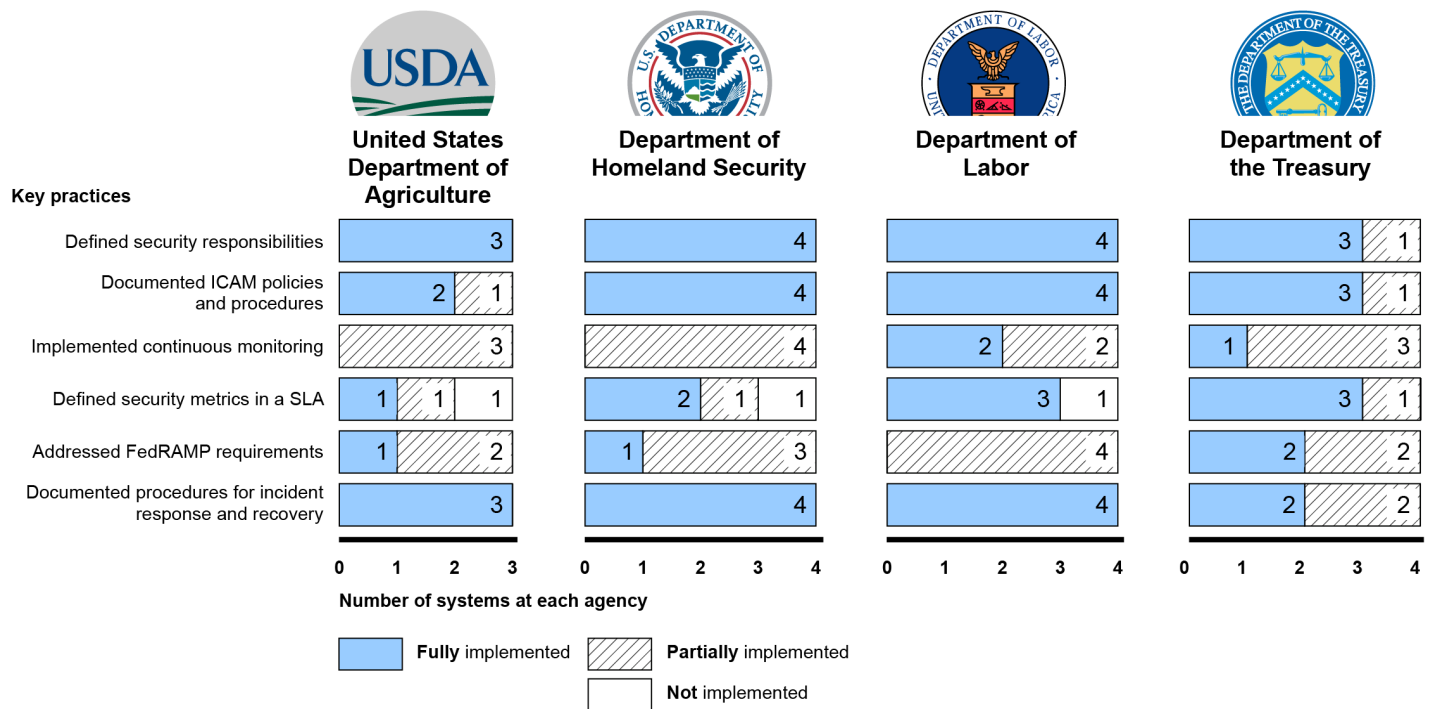
Key practices	United States Department of Agriculture	Department of Homeland Security	Department of Labor	Department of the Treasury
Defined security responsibilities	3	4	4	3 / 1
Documented ICAM policies and procedures	2 / 1	4	4	3 / 1
Implemented continuous monitoring	3	4	2 / 2	1 / 3
Defined security metrics in a SLA	1 / 1 / 1	2 / 1 / 1	3 / 1	3 / 1
Addressed FedRAMP requirements	1 / 2	1 / 3	4	2 / 2
Documented procedures for incident response and recovery	3	4	4	2 / 2

Number of systems at each agency

Legend: Fully implemented, Partially implemented, Not implemented

ICAM (Identity, Credential, and Access Management), SLA (service level agreement), FedRAMP (Federal Risk and Authorization Management Program)

Source: GAO analysis of agency data, and agency logos. | GAO-23-105482

Agencies Defined Security Responsibilities for Nearly All Selected Systems

According to federal guidance,[23] agencies are to define the delineation of security responsibilities between the agency and the CSP. Defining the responsibilities helps agencies to ensure that security roles and functions are fully addressed. To fully implement this practice, an agency should provide evidence that it identified the agency's control implementation

[23]Office of Management and Budget, *Federal Cloud Computing Strategy* (Washington, D.C.: June 24, 2019); and Cybersecurity and Infrastructure Security Agency, U.S. Digital Service, and FedRAMP, *Cloud Security Technical Reference Architecture* (Washington, D.C.: Aug. 2021).

GAO-23-105482 Federal Cloud Environment

responsibilities as well as that of the CSPs for the selected cloud system.[24]

As shown in table 2, the four agencies defined the delineation of security responsibilities for nearly all of the selected systems.

Table 2: Agency Implementation of Defining the Delineation of Security Responsibilities Key Practice

Agency	Selected system, identified by cloud service model[a]	Agency defined the delineation of security responsibilities
Agriculture	PaaS	●
	SaaS system 1	●
	SaaS system 2	●
DHS	IaaS	●
	PaaS	●
	SaaS system 1	●
	SaaS system 2	●
Labor	IaaS	●
	PaaS	●
	SaaS system 1	●
	SaaS system 2	●
Treasury	IaaS	●
	PaaS	●
	SaaS system 1	●
	SaaS system 2	◖

PaaS = Platform as a Service; SaaS = Software as a Service; IaaS = Infrastructure as a Service; DHS = Department of Homeland Security

● = The agency fully implemented the evaluation criteria or practice.

◖ = The agency partially implemented the evaluation criteria or practice.

○ = The agency did not implement the evaluation criteria or practice.

Source: GAO analysis of agency data. | GAO-23-105482

[a]Due to sensitivity concerns, we substituted an identifier based on the cloud service model for the system names.

---

[24]According to FedRAMP's PMO, agencies are to use the control implementation summary developed by the CSP to help identify the controls that the agencies have a primary or shared responsibility to implement. These controls and their implementation should be documented and described in security plans for agency systems that are supported by cloud services.

Three of the four selected agencies (Agriculture, DHS, and Labor) defined the delineation of security responsibilities between the agency and the CSP for each of its selected systems. The fourth agency (Treasury) defined the responsibilities for three of its four selected systems, but did not fully define these responsibilities for its other system.

Specifically, Treasury did not fully define these responsibilities for one of its selected SaaS cloud systems. Although the agency documented its own control responsibilities, it did not fully document the CSP's responsibilities for its SaaS system 2. Treasury officials stated that although the CSP was responsible for the security controls that the agency did not document, they plan to fully document the delineation of responsibilities for this system. However, they did not provide a time frame for when they expect to complete the effort. Until Treasury fully implements the practice, the agency may leave roles and functions unaddressed, which does not ensure operational clarity and that services perform as intended.

Agencies Documented Identity, Credential, and Access Management Policies and Procedures for Nearly All Selected Systems

According to federal guidance,[25] agencies are to document the ICAM policies and procedures for cloud systems. Documenting the policies and procedures helps an agency ensure that the right individual has access to the right resource, at the right time, and for the right reason, in support of the agency's objectives. To fully implement this practice, an agency should document identity and authentication procedures for the cloud system, which include the use of multifactor authentication for organizational users of the cloud system. In addition, the agency should document access control policy and procedures that (1) identified the authorized users of the system, group and role membership, and access authorizations; (2) identified, documented, and defined system access authorizations to support separation of duties; and (3) employed least privilege for specific duties and systems.

---

[25]For example, Office of Management and Budget, *Federal Cloud Computing Strategy: From Cloud First to Cloud Smart* (Washington, D.C.: June 2019); Office of Management and Budget, *Federal Zero Trust Strategy,* OMB Memorandum M-22-09 (Washington, D.C.: Jan. 2022); National Institute of Standards and Technology, *Guidelines on Security and Privacy in Public Cloud Computing*, SP 800-144 (Gaithersburg, MD: Dec. 2011); Office of Management and Budget, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management,* OMB Memorandum M-19-17 (Washington, D.C.: May 21, 2019); Cybersecurity and Infrastructure Security Agency, U.S. Digital Service, and FedRAMP, *Cloud Security Technical Reference Architecture* (Washington, D.C.: Aug. 2021); and General Services Administration, *Federal Cloud Strategy Guide Agency Best Practices for Cloud Migration* (Washington, D.C.: Feb. 2021).

As shown in table 3, the four agencies documented the ICAM policies and procedures for 13 of the 15 selected cloud systems.

Table 3: Agency Implementation of the Identity, Credential, and Access Management Policies and Procedures Key Practice

Agency	Selected system, identified by cloud service model[a]	Agency documented identity and authentication procedures, including multifactor authentication	Agency documented access control policy that identified authorized users, separation of duties, and least privilege	Overall evaluation
Agriculture	PaaS	●	◑	◑
	SaaS system 1	●	●	●
	SaaS system 2	●	●	●
DHS	IaaS	●	●	●
	PaaS	●	●	●
	SaaS system 1	●	●	●
	SaaS system 2	●	●	●
Labor	IaaS	●	●	●
	PaaS	●	●	●
	SaaS system 1	●	●	●
	SaaS system 2	●	●	●
Treasury	IaaS	●	●	●
	PaaS	●	●	●
	SaaS system 1	◑	●	◑
	SaaS system 2	●	●	●

PaaS = Platform as a Service; SaaS = Software as a Service; IaaS = Infrastructure as a Service; DHS = Department of Homeland Security

● = The agency fully implemented the evaluation criteria or practice.

◑ = The agency partially implemented the evaluation criteria or practice.

○ = The agency did not implement the evaluation criteria or practice.

Source: GAO analysis of agency data. | GAO-23-105482

[a]Due to sensitivity concerns, we substituted an identifier based on the cloud service model for the system names.

Two agencies—DHS and Labor—fully documented their ICAM policies and procedures for each of their four selected systems. The other two agencies (Agriculture and Treasury) did not fully document these policies and procedures for one of their selected systems. Specifically,

- Agriculture fully implemented the practice for two systems, and partially implemented the practice for one system.

- Treasury fully implemented the practice for three systems, and partially implemented the practice for one system.

Specifically, Agriculture did not fully document the access authorizations for its PaaS system. Agriculture officials stated that they had defined the access authorizations; however, their access control policy documentation did not include the authorizations. Regarding Treasury, it did not require the use of multifactor authentication for its SaaS system 1. Agency officials stated that they plan to require the use of multifactor authentication; however, they did not provide a time frame for when this requirement would be put in place.

Until Agriculture fully documents the access authorizations, there is an increased potential for abuse of authorized privileges. In addition, users could have access to systems and operate at privilege levels higher than necessary to accomplish organizational missions or business functions. Further, until Treasury requires the use of multifactor authentication, there is an increased risk of unauthorized access to user accounts by malicious actors.

Agencies Partially Implemented Continuous Monitoring Efforts for Most of the Selected Systems

According to federal guidance,[26] agencies are to perform continuous monitoring of their cloud systems. Continuous monitoring helps agencies ensure that their ongoing awareness of the system security and privacy posture supports organizational risk management decisions. To fully implement this practice, an agency should develop and implement a plan for continuously monitoring the security controls that are the agency's responsibility. In addition, an agency should perform periodic (e.g., monthly) reviews of continuous monitoring reports (e.g., security control assessments) from the CSP. Further, an agency should document the use of vulnerability management procedures and tools to monitor the agency's cloud infrastructure and collect and review audit logs, as applicable.

[26]For example, FedRAMP Program Management Office, *FedRAMP Security Assessment Framework*, (Washington, D.C.: Nov. 2017); OMB, *Federal Cloud Computing Strategy: From Cloud First to Cloud Smart* (Washington, D.C.: June 2019); General Services Administration, *FedRAMP Agency Authorization Process: Reusing Authorizations for Cloud Products Quick Guide*, July 26, 2022, *https://www.fedramp.gov/documents-templates/;* Cybersecurity and Infrastructure Security Agency, U.S. Digital Service, and FedRAMP, *Cloud Security Technical Reference Architecture* (Washington, D.C.: Aug. 2021); and National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations,* SP 800-53, Revision 5 (Gaithersburg, MD: Sept. 2020).

However, as shown in table 4, the agencies fully performed continuous monitoring for three of the 15 systems and partially implemented continuous monitoring for the remaining 12 systems.

Table 4: Agency Implementation of Continuous Monitoring Key Practice

Agency	Selected system, identified by cloud service model[a]	Developed and implemented continuous monitoring plan	Reviewed service provider reports	Documented use of vulnerability management tools	Collected and reviewed audit logs	Overall evaluation
Agriculture	PaaS	●	○	●	◐	◐
	SaaS system 1	●	○	N/A[b]	◐	◐
	SaaS system 2	●	○	N/A[b]	N/A[b]	◐
DHS	IaaS	●	◐	●	●	◐
	PaaS	●	◐	●	●	◐
	SaaS system 1	●	◐	●	●	◐
	SaaS system 2	◐	●	N/A[b]	●	◐
Labor	IaaS	◐	●	●	●	◐
	PaaS	●	◐	●	●	◐
	SaaS system 1	●	●	N/A[b]	●	●
	SaaS system 2	●	●	●	●	●
Treasury	IaaS	●	●	●	●	●
	PaaS	◐	◐	●	●	◐
	SaaS system 1	●	○	N/A[b]	N/A[b]	◐
	SaaS system 2	◐	●	○	●	◐

PaaS = Platform as a Service; SaaS = Software as a Service; N/A = not applicable; IaaS = Infrastructure as a Service; DHS = Department of Homeland Security

● = The agency fully implemented the evaluation criteria or practice.

◐ = The agency partially implemented the evaluation criteria or practice.

○ = The agency did not implement the evaluation criteria or practice.

Source: GAO analysis of agency data. | GAO-23-105482

[a]Due to sensitivity concerns, we substituted an identifier based on the cloud service model for the system names.

[b]We assessed as not applicable if the agency documented that it did not have any responsibilities.

One agency—Labor—fully implemented the practice for two of its selected systems and partially implemented the practice for the other two systems. Another agency—Treasury—fully implemented the practice for one of its selected systems and partially implemented the practice for the other three systems. The other agencies (Agriculture and DHS) partially implemented the practice for each of their systems.

With regard to the agencies that partially implemented the practice, Labor developed a plan for continuously monitoring the security controls that are the agency's responsibility for its IaaS system; however, the agency had not implemented the plan. Further, while the agency developed a policy to review the continuous monitoring deliverables in a checklist, the checklist provided was not specific to the cloud services used for its PaaS system.

Treasury developed a plan for continuously monitoring the security controls that are the agency's responsibility for each of its systems; however, the agency had not fully implemented the plans for its PaaS system and SaaS system 2. In addition, the agency provided evidence of steps it had taken to monitor its security controls for SaaS system 2. However, it had not fully assessed the security controls that are the agency's responsibility.

Further, while Treasury officials stated that the agency had reviewed continuous monitoring deliverables from the CSPs, the agency had not performed reviews for its PaaS system and SaaS system 1. Specifically, the agency developed a process for reviewing the deliverables for the PaaS system; however, it did not document the reviews. Moreover, the agency did not document whether it planned to use vulnerability management tools for its SaaS system 2. This was due, in part, to the agency not fully defining the delineation of security responsibilities between the agency and the CSP.

Agriculture did not provide evidence that it had reviewed continuous monitoring deliverables from the CSP for each of its selected systems. Further, while the agency documented the audit logs it planned to collect, and provided example logs for its PaaS system, it did not document its reviews of the logs for its PaaS system and SaaS system 1. Agency officials stated that they plan to improve their process for reviewing the logs. However, they did not provide a time frame for when they expect to complete the effort.

DHS developed a plan for continuously monitoring the security controls that are the agency's responsibility for its SaaS system 2; however, the agency had not fully implemented the plan. Specifically, the agency had not performed annual assessments of the security controls, as required by the continuous monitoring plan. The last assessment performed was in June 2020 and officials stated that they plan to complete the next assessment in 2023. In addition, although the agency reviewed the CSP as part of an annual assessment for its IaaS system, it had not performed

a periodic (e.g., monthly) review of the continuous monitoring deliverables.

Further, although DHS developed processes to review continuous monitoring deliverables, the agency did not document the results of these reviews for its PaaS system or SaaS system 1. For example, the agency stated that the CSP for its PaaS system holds monthly briefings on the continuous monitoring deliverables; however, DHS did not document its review of the deliverables.

One reason agencies have not fully documented their implementation of the continuous monitoring activities is because they did not think it was necessary to do so. However, documenting the implementation of the activities, such as the results from reviews of continuous monitoring deliverables, would provide agencies with greater assurance that they had ongoing awareness of any changes to the security and privacy posture of the system. Until the agencies fully implement each of the continuous monitoring requirements, they will lack information needed to support organizational risk management decisions.

Agencies' Service Level Agreements Defined Security Metrics for Most of the Selected Systems

According to federal guidance,[27] agencies are to have an SLA that defines security metrics with the CSP. SLAs can enable an agency to measure the performance of the services to ensure that it receives the services that it requires. To fully implement this practice, the agency's SLA with the CSP should define (1) performance metrics, (2) how the performance would be measured, and (3) the enforcement mechanisms to ensure the specified performance levels are achieved.

As shown in table 5, the agencies had SLAs that fully defined security metrics for nine of the 15 selected systems.

---

[27]Office of Management and Budget, *Federal Cloud Computing Strategy: From Cloud First to Cloud Smart* (Washington, D.C.: June 2019); Cybersecurity and Infrastructure Security Agency, U.S. Digital Service, and FedRAMP, *Cloud Security Technical Reference Architecture* (Washington, D.C.: Aug. 2021); and General Services Administration, *Federal Cloud Strategy Guide Agency Best Practices for Cloud Migration* (Washington, D.C.: Feb. 2021).

Table 5: Agency Implementation of a Service Level Agreement (SLA) with Cloud Service Provider That Defined Security Metrics Key Practice

Agency	Selected system, identified by cloud service model[a]	SLA defined performance metrics	SLA defined how the performance would be measured	SLA defined the enforcement mechanisms	Overall evaluation
Agriculture	PaaS	●	●	○	◑
	SaaS system 1	○	○	○	○
	SaaS system 2	●	●	●	●
DHS	IaaS	◑	○	○	◑
	PaaS	○	○	○	○
	SaaS system 1	●	●	●	●
	SaaS system 2	●	●	●	●
Labor	IaaS	●	●	●	●
	PaaS	●	●	●	●
	SaaS system 1	●	●	●	●
	SaaS system 2	○	○	○	○
Treasury	IaaS	●	●	●	●
	PaaS	●	●	●	●
	SaaS system 1	●	●	○	◑
	SaaS system 2	●	●	●	●

PaaS = Platform as a Service; SaaS = Software as a Service; IaaS = Infrastructure as a Service; DHS = Department of Homeland Security

● = The agency fully implemented the evaluation criteria or practice.

◑ = The agency partially implemented the evaluation criteria or practice.

○ = The agency did not implement the evaluation criteria or practice.

Source: GAO analysis of agency data. | GAO-23-105482

[a]Due to sensitivity concerns, we substituted an identifier based on the cloud service model for the system names.

None of the agencies fully implemented this practice for all of their selected systems. Two agencies—Labor and Treasury—fully implemented the practice for three of their selected systems, one agency—DHS—fully implemented the practice for two of its selected systems, and the remaining agency—Agriculture—fully implemented the practice for one of its systems.

Specifically,

- Labor did not have an SLA that defined performance metrics for its SaaS system 2, including how they would be measured and the enforcement mechanisms.

- Treasury's SLA for its SaaS system 1 defined performance metrics, including how they would be measured. However, the SLA did not define the enforcement mechanisms to ensure the specified performance levels are achieved.

- DHS's contract for its IaaS system stated that the CSP is to meet its SLAs; however, the agency did not identify the specific SLAs that apply to the system. As a result, it was not clear whether the SLAs defined performance metrics, including how they would be measured, and the enforcement mechanisms. In addition, the agency did not have an SLA that defined performance metrics for its PaaS system, including how they would be measured, and the enforcement mechanisms.

- Agriculture's SLA for its PaaS system defined performance metrics, including how they would be measured. However, the SLA did not define the enforcement mechanisms to ensure the specified performance levels are achieved. In addition, the agency did not have an SLA that defined performance metrics for its SaaS system 1, including how they would be measured, and the enforcement mechanisms.

Agencies provided various reasons for not fully implementing the practice for all of their selected systems, including that the standard SLAs offered by the CSPs did not always define performance metrics, how performance would be measured, or the enforcement mechanisms. Further, officials stated that as a small customer of CSPs, it is difficult to modify the standard SLAs.

Nevertheless, OMB guidance states that agencies should have SLAs with the CSPs to mitigate risk and ensure that services are performed as intended. Until the agencies ensure that their cloud systems have SLAs that define performance metrics, including how the performance would be measured and the enforcement mechanisms, they may be limited in their ability to measure the performance of the services. Consequently, they may not receive the services they require.

Agencies Did Not Fully Address Federal Risk and Authorization Management Program Requirements

According to federal policy and guidance,[28] agencies are to use FedRAMP for cloud systems when conducting risk assessments, security authorizations, and granting ATOs. By using FedRAMP, agencies are able to leverage security authorizations on a government-wide scale to help save costs and the time required to conduct security assessments, and process monitoring reports. To fully implement this practice, an agency should use a CSP with a FedRAMP authorization, and document the agency's: (1) authorization of the cloud system supported by the cloud service; (2) authorization of the cloud services used by the agency, and provide a copy of its authorization letter to the FedRAMP PMO; and (3) the agency's review and risk analysis of the CSP's FedRAMP security package. In addition, the agency's contract with the CSP should require it to comply with FedRAMP security authorization requirements. This is to ensure that a CSP has a contractual obligation to meet and maintain the FedRAMP requirements.

As shown in table 6, the selected agencies fully implemented FedRAMP requirements for four of the 15 selected systems.

Table 6: Agency Implementation of Federal Risk and Authorization Management Program (FedRAMP) Requirements Key Practice

Agency	Selected system, identified by cloud service model[a]	Agency used a CSP that had a FedRAMP authorization	Agency documented authorization of agency system and the cloud service, including its review of CSP's FedRAMP security package	Agency provided authorization letter to the FedRAMP management office	Agency required CSP to comply with FedRAMP requirements	Overall evaluation
Agriculture	PaaS	●	●	●	●	●
	SaaS system 1	●	●	●	◑	◑
	SaaS system 2	●	●	○	○	◑
DHS	IaaS	●	◑	○	●	◑
	PaaS	●	◑	●	●	◑
	SaaS system 1	●	●	●	●	●

[28]Office of Management and Budget, *Security Authorization of Information Systems in Cloud Computing Environments* (Washington, D.C.: Dec. 2011); Cybersecurity and Infrastructure Security Agency, U.S. Digital Service, and FedRAMP, *Cloud Security Technical Reference Architecture* (Washington, D.C.: Aug. 2021); FedRAMP Program Management Office, *FedRAMP Security Assessment Framework* (Washington, D.C.: Nov. 2017); and General Services Administration, *Federal Cloud Strategy Guide Agency Best Practices for Cloud Migration* (Washington, D.C.: Feb. 2021).

Agency	Selected system, identified by cloud service model[a]	Agency used a CSP that had a FedRAMP authorization	Agency documented authorization of agency system and the cloud service, including its review of CSP's FedRAMP security package	Agency provided authorization letter to the FedRAMP management office	Agency required CSP to comply with FedRAMP requirements	Overall evaluation
	SaaS system 2	●	◐	●	○	◐
Labor	IaaS	●	◐	◐	●	◐
	PaaS	●	◐	◐	○	◐
	SaaS system 1	●	◐	◐	●	◐
	SaaS system 2	●	◐	◐	○	◐
Treasury	IaaS	●	●	●	●	●
	PaaS	●	●	●	●	●
	SaaS system 1	●	◐	●	○	◐
	SaaS system 2	●	●	●	○	◐

CSP = cloud service provider; PaaS = Platform as a Service; SaaS = Software as a Service; IaaS = Infrastructure as a Service; DHS = Department of Homeland Security

● = The agency fully implemented the evaluation criteria or practice.

◐ = The agency partially implemented the evaluation criteria or practice.

○ = The agency did not implement the evaluation criteria or practice.

Source: GAO analysis of agency data. | GAO-23-105482

[a]Due to sensitivity concerns, we substituted an identifier based on the cloud service model for the system names.

One agency (Treasury) fully implemented the practice for two of its systems, and two agencies (Agriculture and DHS) fully implemented the practice for one of their selected systems and partially implemented the practice for their other selected systems. The remaining agency (Labor) partially implemented the practice for each of its four selected systems.

With regard to the agency systems that partially implemented the practice, the agencies used a CSP that had a FedRAMP authorization for each of their selected systems. However, the agencies did not always implement the other requirements. Specifically,

- Treasury documented its authorization of the agency system and the cloud service for its SaaS system 1; however, the agency did not document its review and risk analysis of the FedRAMP security package for the CSP used by the agency. In addition, Treasury's

contracts did not require the CSPs to comply with FedRAMP requirements for its SaaS system 1 or SaaS system 2.

- Agriculture officials stated that they were not able to determine whether the agency had provided an authorization letter to FedRAMP PMO for its SaaS system 2. FedRAMP PMO officials stated that they had not received the letter. In addition, Agriculture included requirements in its contract for the CSP to have a FedRAMP authorization at the time of procurement for its SaaS system 1. However, the agency did not include requirements for the CSP to maintain compliance with FedRAMP requirements. Further, the agency's contract did not require the CSP to comply with FedRAMP requirements for its SaaS system 2.

- DHS did not provide evidence that it had issued an authorization for the CSP used by the agency for its IaaS system, PaaS system, and SaaS system 2. Further, DHS officials stated that the agency had provided an authorization letter to the FedRAMP PMO for its IaaS system. However, the agency did not provide supporting evidence and FedRAMP PMO officials stated that they had not received the letter. Further, DHS's contract did not require the CSP to comply with FedRAMP requirements for its SaaS system 2.

- Labor did not provide evidence that it had issued an authorization for the CSPs used by the agency for its IaaS system, PaaS system, and SaaS system 1. In addition, the agency issued an authorization for one of the CSPs used by the agency for its SaaS system 2 and reported that it had issued an authorization for two other CSPs the agency used for the system. However, the agency did not provide supporting documentation. According to agency officials, the authorization for the two CSPs was included as part of the authorization for the system. However, the authorization provided did not include an authorization for these CSPs. Further, the agency did not provide evidence that it had performed a review and risk analysis of the FedRAMP security package for the CSPs used by the agency for its IaaS system or the CSPs used for its SaaS system 2. According to agency officials, they performed a review for both systems, but acknowledged that they did not document the reviews.

In addition, in January 2023, the agency notified the FedRAMP PMO of the agency's authorization of the cloud services for each of the selected systems. However, this notification was after Labor had already authorized the CSPs, and in one case 2 years after. Moreover, Labor's contracts did not require the CSPs to comply with FedRAMP requirements for its PaaS system and SaaS system 2.

Agency officials provided various reasons for not requiring CSPs to comply with FedRAMP requirements in their contracts. For example, Treasury officials stated because they had contracted for FedRAMP authorized cloud services, they did not think it was necessary to also include FedRAMP requirements in the contracts. Further, DHS and Labor officials stated that they considered the FedRAMP process and the FedRAMP authorization for the CSP as sufficient for ensuring that they met requirements. However, OMB policy explicitly states that agencies should ensure that contracts require CSPs to comply with FedRAMP security authorization requirements.[29]

Until the agencies fully implement each of the FedRAMP requirements, they will likely not fully identify the security risk of the system, and ensure they are notified by FedRAMP of any changes to the authorization of the CSP. In addition, there is an increased risk that the CSPs used by the agencies will not fully implement FedRAMP requirements.

Agencies Documented Response and Recovery Procedures for Security and Privacy Incidents for Almost All Selected Systems

According to federal guidance,[30] agencies are to document procedures for responding to and recovering from security and privacy incidents for the cloud system. These procedures help agencies to ensure that they are able to quickly respond to and recover from incidents, and that information resources are protected.

As shown in table 7, the selected agencies documented procedures for responding to and recovering from incidents for almost all of the selected cloud systems.

---

[29]Office of Management and Budget, *Security Authorization of Information Systems in Cloud Computing Environments* (Washington, D.C.: Dec. 8, 2011).

[30]Office of Management and Budget, *Security Authorization of Information Systems in Cloud Computing Environments (*Washington, D.C.: Dec. 2011); National Institute of Standards and Technology, *Guidelines on Security and Privacy in Public Cloud Computing*, SP 800-144 (Gaithersburg, MD: Dec. 2011); Cybersecurity and Infrastructure Security Agency, U.S. Digital Service, and FedRAMP, *Cloud Security Technical Reference Architecture* (Washington, D.C.: Aug. 2021); and General Services Administration, *Federal Cloud Strategy Guide Agency Best Practices for Cloud Migration* (Washington, D.C.: Feb. 2021).

Table 7: Agency Implementation of Documented Procedures for Security and Privacy Incidents Key Practice

Agency	Selected system, identified by cloud service model[a]	Agency documented procedures for security and privacy incidents
Agriculture	PaaS	●
	SaaS system 1	●
	SaaS system 2	●
DHS	IaaS	●
	PaaS	●
	SaaS system 1	●
	SaaS system 2	●
Labor	IaaS	●
	PaaS	●
	SaaS system 1	●
	SaaS system 2	●
Treasury	IaaS	●
	PaaS	●
	SaaS system 1	◐
	SaaS system 2	◐

PaaS = Platform as a Service; SaaS = Software as a Service; IaaS = Infrastructure as a Service; DHS = Department of Homeland Security

● = The agency fully implemented the evaluation criteria or practice.

◐ = The agency partially implemented the evaluation criteria or practice.

○ = The agency did not implement the evaluation criteria or practice.

Source: GAO analysis of agency data. | GAO-23-105482

[a]Due to sensitivity concerns, we substituted an identifier based on the cloud service model for the system names.

Three agencies (Agriculture, Labor, and DHS) documented procedures for responding to and recovering from security and privacy incidents for each of their selected systems. The other agency—Treasury—fully implemented the practice for two selected systems and partially implemented the practice for two systems.

Specifically, Treasury developed incident response plans for its SaaS system 1 and SaaS system 2. However, the agency's plans did not fully document the procedures for recovering from incidents. According to Treasury officials, the contingency plans and procedures for its system are addressed by the agency's IT security program. In addition, officials

stated that the recovery procedures for its SaaS system 2 are addressed by its incident response plan. However, the agency's documentation did not address recovery procedures for the cloud systems.

Without fully documented procedures, the agency could be delayed in responding to and recovering from security or privacy incidents for the selected cloud systems. Furthermore, the agency may not be able to ensure that recovery activities are effective.

Conclusions

As federal agencies increasingly use cloud computing to perform their missions, implementing effective information security controls is a vital part of reducing risks to agency systems. Although none of the agencies fully implemented all of the key practices, three agencies (Agriculture, DHS, and Treasury) fully implemented three practices for most or all of their selected systems, while another agency (Labor) fully implemented four practices for most or all of its systems.

However, the agencies partially implemented or did not implement the other practices for the remaining systems. In particular, all four agencies had one or more systems with shortfalls in implementing continuous monitoring, defining security metrics, and addressing FedRAMP requirements. In addition, two agencies had systems with shortfalls in documenting ICAM policies, while one agency had one or more systems with shortfalls in defining security responsibilities and incident response and recovery procedures. Fully implementing the selected key practices will support the agencies' efforts to ensure the confidentiality, integrity, and availability of agency information in their cloud systems. Further, implementation of these practices will help support the federal government's goal to transform IT through the secure use of cloud services.

Recommendations for Executive Action

We are making a total of 35 recommendations: seven to Agriculture, nine to DHS, nine to Labor, and 10 to Treasury.

The Secretary of Agriculture should ensure that the agency fully documents the access authorizations for its selected PaaS system. (Recommendation 1)

The Secretary of Agriculture should ensure that the agency fully implements continuous monitoring for its selected PaaS system, to include reviewing the continuous monitoring deliverables from the CSP and committing to a time frame to review audit logs. (Recommendation 2)

The Secretary of Agriculture should ensure that the agency fully implements continuous monitoring for its selected SaaS system 1, to include reviewing the continuous monitoring deliverables from the CSP and committing to a time frame to review audit logs. (Recommendation 3)

The Secretary of Agriculture should ensure that the agency fully implements continuous monitoring for its selected SaaS system 2, to include reviewing the continuous monitoring deliverables from the CSP. (Recommendation 4)

The Secretary of Agriculture should ensure that the agency's service level agreements with CSPs define performance metrics, including how they are measured and the enforcement mechanisms. (Recommendation 5)

The Secretary of Agriculture should ensure that the agency provides the authorization letter to the FedRAMP PMO for its selected SaaS system 2. (Recommendation 6)

The Secretary of Agriculture should ensure that the agency's contracts with CSPs include requirements for the service providers to comply with FedRAMP security authorization requirements. (Recommendation 7)

The Secretary of Homeland Security should ensure that the agency fully implements continuous monitoring for its selected SaaS system 2, to include implementing its plans for continuous monitoring of the security controls that are the agency's responsibility. (Recommendation 8)

The Secretary of Homeland Security should ensure that the agency fully implements continuous monitoring for its selected IaaS system, to include performing a regular review of the continuous monitoring deliverables from the CSP. (Recommendation 9)

The Secretary of Homeland Security should ensure that the agency fully implements continuous monitoring for its selected PaaS system, to include implementing its process to review the continuous monitoring deliverables from the CSP. (Recommendation 10)

The Secretary of Homeland Security should ensure that the agency fully implements continuous monitoring for its selected SaaS system 1, to include implementing its process to review the continuous monitoring deliverables from the CSP. (Recommendation 11)

The Secretary of Homeland Security should ensure that the agency's service level agreements with CSPs define performance metrics, including how they are measured and the enforcement mechanisms. (Recommendation 12)

The Secretary of Homeland Security should ensure that the agency fully implements the FedRAMP requirements for its selected IaaS system, to include issuing an authorization for the CSP and providing an authorization letter to the FedRAMP PMO. (Recommendation 13)

The Secretary of Homeland Security should ensure that the agency fully implements the FedRAMP requirements for its selected PaaS system, to include issuing an authorization for the cloud service. (Recommendation 14)

The Secretary of Homeland Security should ensure that the agency fully implements the FedRAMP requirements for its selected SaaS system 2, to include issuing an authorization for the cloud service. (Recommendation 15)

The Secretary of Homeland Security should ensure that the agency's contracts with CSPs include requirements for the service providers to comply with security authorization FedRAMP requirements. (Recommendation 16)

The Secretary of Labor should ensure that the agency fully implements continuous monitoring for its selected IaaS system, to include implementing its plans for continuous monitoring of the security controls that are the agency's responsibility. (Recommendation 17)

The Secretary of Labor should ensure that the agency fully implements continuous monitoring for its selected PaaS system, to include reviewing the continuous monitoring deliverables from the CSP. (Recommendation 18)

The Secretary of Labor should ensure that the agency's service level agreements with CSPs define performance metrics, including how they are measured and the enforcement mechanisms. (Recommendation 19)

The Secretary of Labor should ensure that the agency fully implements the FedRAMP requirements, to include performing a review and risk analysis of the CSPs' FedRAMP security packages for its selected IaaS system. (Recommendation 20)

The Secretary of Labor should ensure that the agency fully implements the FedRAMP requirements, to include issuing an authorization for the cloud service for its selected PaaS system. (Recommendation 21)

The Secretary of Labor should ensure that the agency fully implements the FedRAMP requirements, to include issuing an authorization for the cloud service for its selected SaaS system 1. (Recommendation 22)

The Secretary of Labor should ensure that the agency fully implements the FedRAMP requirements, to include issuing an authorization for each of the cloud services and performing a review and risk analysis of the CSPs' FedRAMP security packages for its selected SaaS system 2. (Recommendation 23)

The Secretary of Labor should ensure that the agency provides authorization letters to the FedRAMP PMO upon issuance of the authorization. (Recommendation 24)

The Secretary of Labor should ensure that the agency's contracts with CSPs include requirements for the service providers to comply with FedRAMP security authorization requirements. (Recommendation 25)

The Secretary of the Treasury should commit to a date for completing efforts to define the delineation of security responsibilities between the agency and the CSP for its selected SaaS system 2. (Recommendation 26)

The Secretary of the Treasury should ensure that the agency commits to a time frame for when it plans to require the use of multifactor authentication for its selected SaaS system 1, and implements the plan. (Recommendation 27)

The Secretary of the Treasury should ensure that the agency fully implements continuous monitoring for its selected PaaS system, to include implementing its plans for continuous monitoring of the security controls that are the agency's responsibility and reviewing the continuous monitoring deliverables from the CSP. (Recommendation 28)

The Secretary of the Treasury should ensure that the agency fully implements continuous monitoring for its selected SaaS system 2, to include implementing its plans for continuous monitoring of the security controls that are the agency's responsibility and documenting the use of

vulnerability management procedures and tools to monitor the agency's cloud infrastructure. (Recommendation 29)

The Secretary of the Treasury should ensure that the agency fully implements continuous monitoring for its selected SaaS system 1, to include reviewing the continuous monitoring deliverables from the CSP. (Recommendation 30)

The Secretary of the Treasury should ensure that the agency's service level agreements with CSPs define the enforcement mechanisms. (Recommendation 31)

The Secretary of the Treasury should ensure that the agency fully implements the FedRAMP requirements, to include performing a review and risk analysis of the CSPs' FedRAMP security packages for its selected SaaS system 1. (Recommendation 32)

The Secretary of the Treasury should ensure that the agency's contracts with CSPs include requirements for the service providers to comply with FedRAMP security authorization requirements. (Recommendation 33)

The Secretary of the Treasury should ensure that the agency fully documents its procedures for responding to and recovering from security and privacy incidents for its SaaS system 1. (Recommendation 34)

The Secretary of the Treasury should ensure that the agency fully documents its procedures for responding to and recovering from security and privacy incidents for its SaaS system 2. (Recommendation 35)

Agency Comments and Our Evaluation

We provided a draft of this report to Agriculture, DHS, Labor, and Treasury for review and comment. In an email, an audit liaison officer in Agriculture's Office of the CIO stated that the agency generally concurred with the findings in our report, but did not say whether the agency agreed or disagreed with our recommendations. Additionally, we received written comments from DHS, Labor, and Treasury that are summarized below. We also received technical comments from DHS, which we have incorporated into the report, as appropriate.

In its written comments (reprinted in appendix III), DHS concurred with our nine recommendations to the agency. Specifically, the agency described ongoing and planned efforts to address two of the nine

recommendations. The agency stated that it expects to complete its efforts regarding continuous monitoring of the security controls that are the agency's responsibility for its selected SaaS system 2 by the end of May 2023. In addition, the agency stated that it expects to complete its efforts to ensure that its contracts with CSPs include requirements for the service providers to comply with security authorization FedRAMP requirements by the end of July 2023.

For the two recommendations regarding the review of continuous monitoring deliverables from the CSP for the IaaS and PaaS systems, the agency stated that it believes it had addressed our recommendations. Specifically, DHS stated that through its role on FedRAMP's Joint Authorization Board,[31] it has performed a regular review of the continuous monitoring deliverables from the CSP. The agency provided additional documentation on its actions. We plan to work with the agency to validate its implementation of these recommendations and, to the extent possible, that the desired results are being achieved.
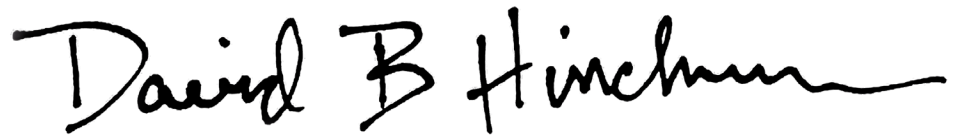
In regards to the recommendation for reviewing the continuous monitoring deliverable reports from the CSP for its SaaS system 1, DHS stated that in addition to the efforts through the Joint Authorization Board, it also reviews the Plans of Actions and Milestones provided by the CSP. However, the documentation the agency provided did not show that it had performed a periodic review of the continuous monitoring deliverables. As a result, we continue to believe that the recommendation is appropriate.

For the recommendation regarding service level agreements, DHS stated it ensures that agency SLAs that define performance metrics are in place whenever possible. For its selected IaaS system, the agency provided a link to a website that includes a list of the CSP's SLAs. However, as noted in our report, the agency did not identify the specific SLAs that apply to the system. In addition, the agency provided an SLA for its PaaS system. However, as noted in our report, the SLA did not define performance metrics, including how they are measured and the enforcement mechanisms. As a result, we continue to believe that the recommendation is appropriate.

---

[31]The Joint Authorization Board is the primary governance and decision-making body for the FedRAMP program. The board reviews and provides provisional security authorizations of cloud solutions using a standardized baseline approach. The chief information officers from the Department of Defense, Department of Homeland Security, and General Services Administration serve on the board.

For the three recommendations regarding FedRAMP requirements, the agency stated it ensures the CSPs meet FedRAMP requirements through its role on FedRAMP's Joint Authorization Board. In particular, the agency stated that as one of the board's members, it had authorized and signed the FedRAMP ATOs for the CSPs. The agency provided additional documentation on its actions. We plan to work with the agency to validate its implementation of these recommendations and, to the extent possible, that the desired results are being achieved.

In Labor's written comments (reprinted in appendix IV), the agency neither agreed nor disagreed with its nine recommendations. Specifically, Labor described its plans to address the recommendation to ensure that the agency's contracts with CSPs include requirements for the service providers to comply with FedRAMP security authorization requirements. The agency stated that it would add a clause into the standard cybersecurity language, which, according to Labor, it inserts into every contracting action. The agency estimated that it would complete its efforts by the end of fiscal year 2023.

The agency further stated that it believed that it had addressed the other eight recommendations. Specifically, Labor described actions it had taken to address the two recommendations for continuous monitoring for its selected IaaS and PaaS systems. The agency also described actions it had taken to address the recommendation regarding SLAs and the four recommendations regarding FedRAMP requirements. The agency provided additional documentation on its actions. We plan to work with the agency to validate its implementation of these recommendations and, to the extent possible, that the desired results are being achieved.

Moreover, Labor stated that it had addressed our recommendation to provide authorization letters to the FedRAMP PMO upon issuance of the authorization. The agency stated that it had sent an authorization letter to the FedRAMP PMO on January 19, 2023. However, as discussed in our report, this notification was after Labor had already authorized the CSPs, and in one case 2 years after. As a result, we continue to believe that the recommendation is appropriate.

Finally, in its written comments (reprinted in appendix V), Treasury concurred with the findings for its SaaS system 2 and described its plans to implement the four recommendations for this system. The agency did not provide any comments on the remaining six recommendations.

We are sending copies of this report to the appropriate congressional committees, the Director of the Office of Management and Budget, the secretaries and agency heads of the departments and agencies addressed in this report, and other interested parties. In addition, this report will be available at no charge on the GAO website at http://www.gao.gov.

Should you or your staffs have any questions on information discussed in this report, please contact Dave Hinchman at (214) 777-5719 or HinchmanD@gao.gov; or Brian Bothwell (202) 512-6888 or BothwellB@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix VI.

David B. Hinchman
Director, Information Technology and Cybersecurity

Brian Bothwell
Director, Science, Technology Assessment, and Analytics

Appendix I: Participants in the Expert Panels

In January 2022 and April 2022 we held expert panels with public and private sector experts on cloud security. The purpose of the discussions was to gain the panels' input on existing guidance and policies on cloud security. At both panels we presented a list of existing policies and guidance to determine if there were any other cloud security sources to consider. We also received confirmation on the policies and guidance they considered to be most useful. The panelists provided valuable input which helped us to identify the relevant guidance that we then used to identify the key practices identified in this report. However, the panelists were not involved in the selection or review of the key practices. Table 8 provides the panel participants, all of whom indicated they wished to be acknowledged.

Table 8: Public and Private Sector Panel Participants

Name	Organization
Public sector panel – January 2022	
Christopher Bollerer	Department of Health and Human Services
Joseph Fourcade	Department of Veterans Affairs
Steven Hernandez	Department of Education
Beau Houser	Census Bureau
Ray O'Brien	National Aeronautics and Space Administration
Elizabeth Schweinsberg	U.S. Digital Service
John Simms	Department of Homeland Security, Cybersecurity and Infrastructure Security Agency
Greg Sisson	Department of Energy
Dr. Mark Stanley	Department of Defense
McKay Tolboe	Department of Defense
Leo Wong	Federal Trade Commission
Private sector panel – April 2022	
Grant Dasher	Google (formerly)
Taher ElGamal	Salesforce
Jim Jennis	Amazon Web Services (formerly)
Anil Ramcharan	Deloitte
Scott Robertson	IBM
Dr. Mari Spina	MITRE Corporation
John Walton	Microsoft
Von Welch	Indiana University
Phil White	Center of Internet Security

Source: GAO cloud security guidance panel information. | GAO-23-105482

Appendix II: Objective, Scope, and Methodology

Our objective was to evaluate the extent to which selected agencies have effectively implemented key cloud security practices. To address our objective, we identified a nongeneralizable sample of four Chief Financial Officers Act agencies that currently use cloud services.[1] To select the agencies, we analyzed federal IT Dashboard data, and totaled the number of IT investments that agencies reported were leveraging cloud computing for fiscal year 2021 (i.e., cloud investments). We excluded agencies that we had assessed in a recent related report.[2] In addition, we excluded the Department of Defense because we had an ongoing review of the agency's use of cloud services.[3]

We then organized the agencies into two groups: agencies with 50 or more cloud investments and agencies with fewer than 50 cloud investments. We selected the two agencies with the highest number of cloud investments from each group. This resulted in a selection of four agencies—the Departments of Agriculture, Homeland Security (DHS), Labor, and the Treasury.

In addition, we selected cloud systems from each of the agencies. To select these systems, we requested the selected agencies to provide an inventory of its cloud systems. We then selected a random sample of four cloud systems from three of the four agencies (DHS, Labor, and Treasury), and three cloud systems from one agency (Agriculture).[4] To

---

[1]The 24 agencies covered by the *Chief Financial Officers Act of 1990* are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Personnel Management; Small Business Administration; Social Security Administration; and the U.S. Agency for International Development (31 U.S.C. § 901(b)).

[2]In GAO-20-126, we assessed the extent to which four agencies—the Department of Health and Human Services, the General Service Administration, the Environmental Protection Agency, and the U.S. Agency for International Development—had addressed key elements of the Federal Risk and Authorization Management Program's authorization process. Thus, we excluded these four agencies from our review.

[3]GAO, *Cloud Computing: DOD Needs to Improve Workforce Planning and Software Application Modernization,* GAO-22-104070 (Washington, D.C.: June 29, 2022).

[4]We initially selected four systems from Agriculture; however, during our review, Agriculture transferred responsibility for one selected system to the General Services Administration. Since Agriculture no longer had security responsibilities for the system, we removed the system from our review. Based on our engagement timelines, we decided to not select a new system for our evaluation. As a result, our review for Agriculture only included three cloud systems.

ensure that we evaluated a broad range of services, for each agency, we selected one Infrastructure as a Service (IaaS), one Platform as a Service (PaaS), and two Software as a Service (SaaS) cloud systems. We selected two SaaS services because this cloud service model represented the most cloud systems of the three models for the selected agencies. Further, we did not select cloud systems that used a private cloud deployment model. In addition, due to sensitivity concerns, we are not disclosing the names of the systems in this report. Instead, we refer to the selected systems by the service model.

To determine the reliability of inventories, we reviewed the data for obvious errors and for completeness. We also interviewed agency officials to corroborate the data. We determined that the data were sufficiently reliable for the purposes of this report, which were to select cloud systems from each agency and assess the extent to which agencies implemented key cloud security practices for each system. To identify key cloud security practices, we first identified federal IT policies (e.g., federal cloud strategy) and federal guidance (e.g., the Cloud Security Technical Reference Architecture) relevant to securing cloud systems.[5]

To help in identifying the relevant guidance, we held two expert panels to discuss these and other cloud security guidance. Specifically, in January 2022 we held an expert panel with public sector experts and in April 2022 we held a panel with private sector experts. The meeting of experts in the private sector was planned and convened with the assistance of the National Academy of Science to better ensure that a breadth of expertise was brought to bear in its preparation; however, we were responsible for all final decisions regarding meeting substance and expert participation.

At both panels we presented a list of existing policies and guidance to these experts to determine if there were any other cloud security sources to consider. We also received confirmation on the policies and guidance they considered to be most useful. Appendix I lists the participants and their corresponding organizations from both panels.

---

[5]Office of Management and Budget, *Federal Cloud Computing Strategy: From Cloud First to Cloud Smart* (Washington, D.C.: June 2019); and Cybersecurity and Infrastructure Security Agency, U.S. Digital Service, and FedRAMP, *Cloud Security Technical Reference Architecture* (Washington, D.C.: Aug. 2021).

We then analyzed the relevant guidance to identify practices that
agencies should apply to their cloud systems. From this review, we
selected the following six key cloud security practices:

1. Define the delineation of security responsibilities between the agency
   and the cloud service provider (CSP) for the cloud system.

2. Document the identity, credential, and access management (ICAM)
   policies and procedures for the cloud system.

3. Develop and implement a plan for continuously monitoring the cloud
   system.

4. Define security metrics in a service level agreement with the CSP.

5. Use the Federal Risk and Authorization Management Program
   (FedRAMP) when conducting risk assessments and security
   authorizations and when granting an authority to operate (ATO) for
   the cloud system.

6. Document procedures for responding to and recovering from security
   and privacy incidents for the cloud system.

In addition, we reviewed the supporting policies and guidance for each
key practice and identified specific evaluation criteria for each key
practice (see table 9).

Table 9: Evaluation Criteria Associated with the Key Cloud Security Practices

Key practice	Evaluation criteria
Define the delineation of security responsibilities between the agency and the cloud service provider (CSP) for the cloud system.	• The agency identified its control implementation responsibilities as well as that of the CSPs.
Document the identity, credential, and access management (ICAM) policies and procedures for the cloud system.	• The agency documented identity and authentication procedures for the cloud system, including the use of multifactor authentication for organizational users of the cloud system. • The agency documented access control policy and procedures that: (1) identified the authorized users of the system, group and role membership, and access authorizations; (2) identified, documented, and defined system access authorizations to support separation of duties; and (3) employed least privilege for specific duties and systems.
Develop and implement a plan for continuously monitoring the cloud system.	• The agency developed and implemented a plan for continuously monitoring the security controls that are the agency's responsibility. • The agency reviewed continuous monitoring deliverables from the CSP. • The agency documented the use of vulnerability management procedures and tools to monitor the agency's cloud infrastructure. • The agency collected and reviewed audit logs.

Key practice	Evaluation criteria
Define security metrics in a service level agreement (SLA) with the CSP.	• The agency's SLA with the CSP defined performance metrics. • The agency's SLA with the CSP defined how the performance would be measured. • The agency's SLA with the CSP defined the enforcement mechanisms to ensure the specified performance levels are achieved.
Use FedRAMP when conducting risk assessments, security authorizations, and granting an authority to operate for the cloud system.	• The agency leveraged a CSP that had a FedRAMP authorization. • The agency documented the authorization of (1) the agency system supported by the cloud service and (2) the cloud service used by the agency. • The agency provided a copy of its authorization letter for the cloud service (cloud service authorization letter) to the FedRAMP Program Management Office. • The agency's contract required the CSP to comply with FedRAMP security authorization requirements.
Document procedures for responding to and recovering from security and privacy incidents for the cloud system.	The agency documented procedures for responding to and recovering from security and privacy incidents for the cloud system.

FedRAMP = Federal Risk and Authorization Management Program

Source: GAO analysis of federal policies and guidance. | GAO-23-105482

We then obtained documentation from each agency, including system security plans, contracts, incident response plans, and contingency plans. We analyzed these documents to determine whether the agency had implemented the six key practices for each of the agency's selected cloud systems. For each system, we first assessed each agency's implementation of our evaluation criteria within each key practice as:

• fully implemented—the agency provided evidence which showed that it fully or largely addressed the elements of the criteria.

• partially implemented—the agency provided evidence that showed it had addressed at least part of the criteria.

• not implemented—the agency did not provide evidence that it had addressed any part of the criteria.

To determine an overall rating for each of the six key cloud security practices for an individual system, we then summarized the results of our assessments of the evaluation criteria by assessing each key practice as:

• fully implemented—the agency provided evidence that showed that it fully implemented each evaluation criteria.

- partially implemented—the agency provided evidence that showed it had partially or fully implemented at least one or more of the evaluation criteria, but did not fully implement each criteria.

- not implemented—the agency did not provide evidence that it had implemented any part of the evaluation criteria.

We supplemented our analysis with interviews of relevant agency officials about their efforts to implement the key cloud security practices.

We conducted this performance audit from October 2021 to May 2023 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix III: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

April 28, 2023

David Hinchman
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Brian Bothwell
Director, Science, Technology Assessment, and Analytics
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Management Response to Draft Report GAO-23-105482, "CLOUD SECURITY: Selected Agencies Need to Fully Implement Key Practices"

Dear Messrs. Hinchman and Bothwell:

Thank you for the opportunity to comment on this draft report. The U.S. Department of Homeland Security (DHS or the Department) appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing this report.

DHS leadership is pleased to note GAO's positive recognition of the work being done by the Department to address possible vulnerabilities regarding cloud security. DHS remains committed to implementing effective information security controls that makes our cloud computing systems safer.

The draft report contained 35 recommendations, including 9 for DHS with which the Department concurs. Enclosed find our detailed response to each recommendation. DHS previously submitted technical comments addressing several accuracy, contextual, and other issues under a separate cover for GAO's consideration.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Sincerely,

JIM H CRUMPACKER
Digitally signed by JIM H CRUMPACKER
Date: 2023.04.28 13:23:49 -04'00'

JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Enclosure

2

**Enclosure: Management Response to Recommendations
Contained in GAO-23-105482**

GAO recommended that the Secretary of Homeland Security:

Recommendation 8: Ensure that the agency fully implements continuous monitoring for
its selected SaaS [Software as a Service] system 2, to include implementing its plans for
continuous monitoring of the security controls that are the agency's responsibility.

Response: Concur. DHS Office of the Chief Information Officer (OCIO) has already
taken steps to address the issue. DHS adjusted assessment schedules from legacy 3-year
complete assessments to one aligned with FedRAMP annual assessment and continuous
monitoring requirements. The formal approval process is currently ongoing. Once
approved, DHS will request formal recommendation closure. Estimated Completion
Date (ECD): May 31, 2023.

Recommendation 9: Ensure that the agency fully implements continuous monitoring for
its selected IaaS [Infrastructure as a Service] system, to include performing a regular
review of the continuous monitoring deliverables from the CSP [cloud service provider].

Response: Concur. DHS performs full, thorough, regular, and ongoing continuous
monitoring activities with this CSP through its responsibility and activities on the
FedRAMP Joint Authorization Board (JAB). All continuous monitoring deliverables are
regularly reviewed and analyzed, and the JAB engages with this CSP for all required
vulnerability, change, inventory, remediation, escalation, incident, and directive
management activities. U.S. Immigration and Customs Enforcement (ICE) regularly
reviews the CSP's continuous monitoring deliverables. During the fieldwork phase, ICE
provided GAO with the remediation plans, reports, meeting minutes, and meeting stakeholder
participants to demonstrate compliance.

DHS also met with GAO on April 6, 2023 to discuss draft recommendations and at their request
on April 12, 2023 provided additional artifacts of the continuous monitoring and performance
management, review, analysis, and adjudication of CSP deliverables performed by the DHS
CIO through JAB activities.

We request that GAO consider this recommendation resolved and closed, as implemented.

Recommendation 10: Ensure that the agency fully implements continuous monitoring
for its selected PaaS [Platform as a Service] system, to include implementing its process
to review the continuous monitoring deliverables from the CSP.

3

Response: Concur. DHS performs full, thorough, regular, and ongoing continuous monitoring activities with this CSP through its responsibility and activities on the FedRAMP JAB. All continuous monitoring deliverables are regularly reviewed and analyzed, and the JAB engages with this CSP for all required vulnerability, change, inventory, remediation, escalation, incident, and directive management activities. Transportation Security Administration (TSA) Information Technology performs reviews and analysis of all its CSPs via continuous monitoring.

DHS also met with GAO on April 6, 2023 to discuss draft recommendations and at their request on April 12, 2023 provided additional artifacts of the continuous monitoring and performance management, review, analysis, and adjudication of CSP deliverables performed by the DHS CIO through JAB activities.

We request that GAO consider this recommendation resolved and closed, as implemented.

Recommendation 11: Ensure that the agency fully implements continuous monitoring for its selected SaaS system 1, to include implementing its process to review the continuous monitoring deliverables from the CSP.

Response: Concur. U.S. Customs and Border Protection (CBP) agrees with the importance of ensuring continuous monitoring and already has in place a process which sufficiently addresses the intent of this recommendation. CBP, Office of Information and Technology (OIT) already implemented a process to review the continuous monitoring deliverable SOC 1 Reports, which are provided by the CSP, Amazon Web Services (AWS).

Specifically, CBP routinely receives SOC 1 reports from AWS on their 6-month standard and 9-month federal government schedules. These SOC 1 reports are downloaded and disseminated to various CBP offices, as appropriate. CBP OIT reviews and analyzes all complimentary user entity controls contained in each SOC 1 Report and formally documents any observations. If there are any high-risk findings, CBP OIT submits their observations back to the CSP. Finally, CBP OIT also reviews the Plans of Action and Milestones provided by the CSP.

DHS also met with GAO on April 6, 2023 to discuss draft recommendations and at their request on April 12, 2023 provided additional artifacts of the continuous monitoring and performance management, review, analysis, and adjudication of CSP deliverables performed by the DHS CIO through JAB activities.

We request that GAO consider this recommendation resolved and closed, as implemented.

4

Recommendation 12: Ensure that the agency's service level agreements with CSPs define performance metrics, including how they are measured and the enforcement mechanisms.

Response: Concur. DHS OCIO ensures that agency service level agreements (SLA) that define performance metrics are in place whenever possible. Some of the DHS CSPs (especially hyper scale providers) have Advertised Service Levels (ASL) with performance metrics and enforcement/consequence mechanisms defining the CSP's committed service level and the consequences/remunerations for not meeting their advertised service levels. They are set unilaterally by the CSP and are not always SLAs set by contractual agreements but serve the same purpose. If DHS determines the ASL is adequate for mission needs and includes performance metrics and enforcement mechanisms, it is functionally the same. Many contracts for such offerings are with resellers or brokers and would not or could not contractually enforce an SLA with the CSP, but it may be the only available option. For those CSPs with whom DHS has contracted directly, DHS has included SLAs and should whenever possible, which define performance metrics, including how they are measured and enforced where that makes sense.

DHS also met with GAO on April 6, 2023 to discuss draft recommendations and at their request on April 12, 2023 provided additional artifacts of the ASLs for the requested CSPs.

We request that GAO consider this recommendation resolved and closed, as implemented.

Recommendation 13: Ensure that the agency fully implements the FedRAMP requirements for its selected IaaS system, to include issuing an authorization for the CSP and providing an authorization letter to the FedRAMP Program Management Office.

Response: Concur. DHS ensures that FedRAMP requirements are met, including issuing an authorization for FedRAMP-authorized CSPs and enabling documented inheritance of security controls provided by the CSP through the DHS Governance, Records, and Compliance (GRC) system. Through its responsibilities and activities on the FedRAMP JAB when issuing authorizations, DHS ensures that the CSP meets all FedRAMP and Federal requirements with no unmitigated Critical or High findings. Risk analysis is performed by DHS, certified by the JAB Technical Representative, and JAB provisional Authority to Operate (P-ATOs) are ultimately authorized and signed by the DHS Chief Information Officer as one of three JAB Authorizing Officials who make authorization decisions. ICE also maintains an ATO for the CSPs as part of the ICE Cloud General Support System ATO.

DHS also met with GAO on April 6, 2023 to discuss draft recommendations and at their request on April 12, 2023 provided additional artifacts of the documented issuance of authorization for the CSP, the documented inheritance of the authorized system(s) as well as the JAB

5

authorization signed by the DHS CIO and the Certification Memo signed by the DHS Technical Representative / Risk Executive.

We request that GAO consider this recommendation resolved and closed, as implemented.

Recommendation 14: Ensure that the agency fully implements the FedRAMP requirements for its selected PaaS system, to include issuing an authorization for the cloud service.

Response: Concur. DHS ensures that FedRAMP requirements are met, including issuing an authorization for FedRAMP-authorized CSPs and enabling documented inheritance of security controls provided by the CSP through the DHS GRC. Through its responsibilities and activities on the FedRAMP JAB when issuing authorizations, DHS ensures that the CSP meets all FedRAMP and federal requirements with no unmitigated Critical or High findings. Risk analysis is performed by DHS, certified by the JAB Technical Representative, and JAB P-ATOs are ultimately authorized and signed by the DHS CIO as one of three JAB Authorizing Officials who make authorization decisions. The TSA system inherited from the authorized CSP is also fully authorized by TSA's Authorizing Official and documented in the DHS Cyber Security Assessment and Management system (CSAM).

DHS also met with GAO on April 6, 2023 to discuss draft recommendations and at their request on April 12, 2023 provided additional artifacts of the documented issuance of authorization for the CSP, the documented inheritance of the authorized system(s) as well as the JAB authorization signed by the DHS CIO and the Certification Memo signed by the DHS Technical Representative / Risk Executive.

We request that GAO consider this recommendation resolved and closed, as implemented.

Recommendation 15: Ensure that the agency fully implements the FedRAMP requirements for its selected SaaS system 2, to include issuing an authorization for the cloud service.

Response: Concur. DHS ensures that FedRAMP requirements are met, including issuing an authorization for FedRAMP-authorized CSPs and enabling documented inheritance of security controls provided by the CSP through the DHS GRC. Through its responsibilities and activities on the FedRAMP JAB when issuing authorizations, DHS ensures that the CSP meets all FedRAMP and federal requirements with no unmitigated Critical or High findings. Risk analysis is performed by DHS, certified by the JAB Technical Representative, and JAB P-ATOs are ultimately authorized and signed by the DHS CIO as one of three JAB Authorizing Officials who make authorization decisions. The DHS system inherited from the authorized CSP is also fully authorized and documented in the DHS CSAM.

6

DHS also met with GAO on April 6, 2023 to discuss draft recommendations and at their request on April 12, 2023 provided additional artifacts of the documented issuance of authorization for the CSP, the documented inheritance of the authorized system(s) as well as the JAB authorization signed by the DHS CIO and the Certification Memo signed by the DHS Technical Representative / Risk Executive.

We request that GAO consider this recommendation resolved and closed, as implemented.

Recommendation 16: Ensure that the agency's contracts with CSPs include requirements for the service providers to comply with security authorization FedRAMP requirements.

Response: Concur. DHS OCIO has incorporated contractual language for compliance with FedRAMP authorization requirements into the Information Technology Acquisition Review (ITAR) process for classified and unclassified procurements. The ITAR process provides the requirements that must be included in acquisition documents for information systems that are hosted, operated, maintained, and used on behalf of DHS. The current ITAR process requirement states, "All procurement of Cloud services must comply with the FedRAMP Authorization Act as part of the FY23 National Defense Authorization Act." Additionally, the ITAR requirements and contract language are being updated to include additional detail and clarifying requirements specifying compliance with FedRAMP authorization requirements. ECD: July 31, 2023.

7

Appendix IV: Comments from the Department of Labor

U.S. Department of Labor

Office of the Assistant Secretary
for Administration and Management
Washington, D.C. 20210

April 20, 2023

David Hinchman
Director, Information Technology and Cybersecurity
Government Accountability Office
441 G Street, NW
Washington, D.C. 20548

Dear Director Hinchman:

Thank you for the opportunity to review and comment on draft report *Cloud Security: Selected Agencies Need to Fully Implement Key Practices" (GAO-23-105482, Job Code 105482).* We appreciate the Government Accountability Office's (GAO) efforts and insights.

Recommendation 17: *The Secretary of Labor should ensure that the agency fully implements continuous monitoring for its selected IaaS system, to include implementing its plans for continuous monitoring of the security controls that are the agency's responsibility.*

DOL Response: The Office of the Chief Information Office (OCIO) has verified that annual assessments of third-party providers, including cloud service providers, are formally documented, reviewed, and signed by appropriate levels of management. As a part of the Department of Labor's (DOL) information security continuous monitoring (ISCM) program, an Annual Security Assessment Plan is issued to agencies each year that outlines a plan to conduct security assessment testing. In Fiscal Year (FY) 23, DOL implemented monthly ISCM oversight/reporting to validate adherence ISCM requirements. OCIO believes this recommendation has been addressed.

Recommendation 18: *The Secretary of Labor should ensure that the agency fully implements continuous monitoring for its selected PaaS system, to include reviewing the continuous monitoring deliverables from the CSP.*

DOL Response: In January 2023, DOL issued the Cybersecurity Policy Portfolio (CPP). Cloud Service Provider and FedRAMP requirements are documented throughout the CPP volumes. As a part of OCIO's information security continuous monitoring (ISCM) program, DOL performs monthly ISCM oversight to validate adherence ISCM requirements. OCIO believes this recommendation has been addressed.

Recommendation 19: *The Secretary of Labor should ensure that the agency's service level agreements with CSPs define performance metrics, including how they are measured, and the enforcement mechanisms.*

DOL Response: DOL ensures CSP SLAs are satisfactory and measurable, and meet DOL standards. This is done by reviewing the SLAs as defined by the CSPs. First step is understanding what the SLAs are by service, as they do vary within the CSP. We then gather any outage evidence and submit to the CSP as a breach of SLA. After its analyzed by the CSP, and

SLAs were found to indeed been breached we (DOL) will receive credits commensurate to the level and duration of the outage. OCIO believes this recommendation has been addressed.

Recommendation 2*0*: *The Secretary of Labor should ensure that the agency fully implements the FedRAMP requirements, to include performing a review and risk analysis of the CSP's FedRAMP security packages for its selected IasS system.*

DOL Response: In January 2023, DOL issued the Cybersecurity Policy Portfolio (CPP). Volume 4 of the CPP (Assessment, Authorization, and Monitoring) notes that for FedRAMP Cloud Service Providers (CSPs), annual review of 3PAO assessment results is sufficient to document continuous monitoring for CSP-provided controls. For DOL-implemented controls, monitoring occurs in accordance with the DOL ISCM Plan. Additionally, DOL implemented monthly ISCM oversight/reporting at the beginning of FY23 to validate adherence to ISCM requirements. OCIO believes this recommendation has been addressed.

Recommendation 21: *The Secretary of Labor should ensure that the agency fully implements the FedRAMP requirements, to include issuing an authorization for the cloud service for its selected PaaS system.*

DOL Response: An authorization letter, signed by the Authorizing Official, confirmed a review and authorization of the applicable FedRAMP authorization packages. A copy of the authorization letter was sent to the FedRAMP Program Management Office January 19, 2023. A copy of the authorization letter was also provided to GAO January 31, 2023. OCIO believes this recommendation has been addressed.

Recommendation 22: *The Secretary of Labor should ensure that the agency fully implements the FedRAMP requirements, to include issuing an authorization for the cloud service for its selected SaaS system 1.*

DOL Response: An authorization letter, signed by the Authorizing Official, confirmed a review and authorization of the applicable FedRAMP authorization packages. A copy of the authorization letter was sent to the FedRAMP Program Management Office January 19, 2023. A copy of the authorization letter was also provided to GAO January 31, 2023. OCIO believes this recommendation has been addressed.

Recommendation 23: *The Secretary of Labor should ensure that the agency fully implements the FedRAMP requirements, to include issuing an authorization for each of the cloud services and performing a review and risk analysis of the CSP's FedRAMP security packages for its selected SaaS system 2.*

DOL Response: In January 2023, DOL issued the Cybersecurity Policy Portfolio (CPP). Volume 4 of the CPP (Assessment, Authorization, and Monitoring) notes that for FedRAMP Cloud Service Providers (CSPs), annual review of 3PAO assessment results is sufficient to document continuous monitoring for CSP-provided controls. For DOL-implemented controls, monitoring occurs in accordance with the DOL ISCM Plan. Additionally, DOL implemented

monthly ISCM oversight/reporting at the beginning of FY23 to validate adherence to ISCM requirements. OCIO believes this recommendation has been addressed.

Recommendation 24: *The Secretary of Labor should ensure that the agency provides authorization letters to the FedRAMP Program Management Office upon issuance of the authorization.*

DOL Response: An authorization letter, signed by the Authorizing Official, confirmed a review and authorization of the applicable FedRAMP authorization packages. A copy of the authorization letter was sent to the FedRAMP Program Management Office January 19, 2023. A copy of the authorization letter was also provided to GAO January 31, 2023. OCIO believes this recommendation has been addressed.

Recommendation 25: *The Secretary of Labor should ensure that the agency's contracts with CSPs include requirements for the service providers to comply with FedRAMP security authorization requirements.*

DOL Response: The Cybersecurity Directorate will add this clause into the standard cybersecurity language, which is inserted into every contracting action. This is estimated to be completed by FY23 Q4.

Should you have any questions regarding the Department's response, please have your staff contact Gundeep Ahluwalia, Chief Information Officer, at (202) 693-4200.

Sincerely,

Rachana Desai Martin
Assistant Secretary for
Administration and Management

Appendix V: Comments from the Department of the Treasury

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

April 25, 2023

David B. Hinchman
Director, Information Technology and Cybersecurity
General Accountability Office
441 G St., NW
Washington, DC 20548

Thank you for the opportunity to review the Government Accountability Office (GAO)'s draft report entitled "Cloud Security: Selected Agencies Need to Fully Implement Key Practices (GAO-23-105482). For this engagement, GAO selected four of Treasury's cloud-based systems – one from the Bureau of Fiscal Service (BFS), the Internal Revenue Service (IRS), the U.S. Mint, and the Alcohol and Tobacco Tax and Trade Bureau (TTB).

We appreciate the work performed by your team, and the Recommendations provided. IRS, BFS, and the U.S. Mint have no additional comments. TTB submitted comments, which are attached. Once the finalized report is released, Treasury will develop Planned Corrective Actions as appropriate.

If you have any further questions, please direct your staff to contact the Office of the CIO directly.

Respectfully,

Antony P.
Arcadi

Antony P. Arcadi
2023.04.25
16:47:03 -04'00'

Tony Arcadi
Deputy Assistant Secretary for Information Systems
and Chief Information Officer

ATTACHMENT

1. GAO Cloud Security - Treasury SaaS System 2 Response-Final

GAO 105482 – "Cloud Security: Selected Agencies Need to Fully Implement Key Practices"

Responses from Treasury Alcohol and Tobacco Tax and Trade Bureau (TTB)

For: *Treasury SaaS System 2*

Key practice 1 – one partial compliant

Response: Treasury concurs and will fully document and delineate the Cloud Service Provider (CSP) and the customer responsibilities for SaaS System 2.

Key practice 2 – fully compliant

Response: No comment.

Key practice 3 – one partial compliant, one non-compliant

Response:

Treasury reviews vendor vulnerability scan, security control, security assessment, and POA&M documentation provided by FedRAMP for SaaS System 2 on an annual basis according to its Cloud Authority to Operate (ATO) process. In conjunction with the actions for key practice 1, Treasury will fully document and delineate its security control responsibilities for SaaS System 2.

Treasury will also fully document that the CSP has vulnerability management responsibilities for SaaS System 2, and that Treasury follows the Cloud ATO Process to review the CSP's vulnerability reports annually.

Key practice 4 – fully compliant

Response: No comment.

Key practice 5 – one non-compliant

Response: Treasury concurs. Treasury's recently awarded TCloud contract includes language that satisfies this recommendation. As existing contracts migrate to TCloud, they will inherit the language from the base contract.

Key practice 6 – one partial compliant

Response: Treasury concurs and will fully document recovery procedures for SaaS System 2.

Appendix VI: GAO Contacts and Staff Acknowledgments

GAO Contacts

David B. Hinchman at (214) 777-5719, HinchmanD@gao.gov

Brian Bothwell at (202) 512-6888, BothwellB@gao.gov

Staff Acknowledgments

In addition to the contacts named above, the following staff made key contributions to this report: Neelaxi Lakhmani (Assistant Director), John Ortiz (Assistant Director), Scott Borre (Analyst in Charge), Alina Budhathoki, Christopher Businsky, Rebecca Eyler, Jennifer Leotta, Sejal Sheth, Priscilla Smith, and Andrew Stavisky.