United States Government Accountability Office

Report to Congressional Committees

June 2026

CYBERSECURITY

Selected Agencies Need to Better Protect Cloud Data

GAO-26-108443

GAO Highlights

CYBERSECURITY

Selected Agencies Need to Better Protect Cloud Data

GAO-26-108443 June 2026

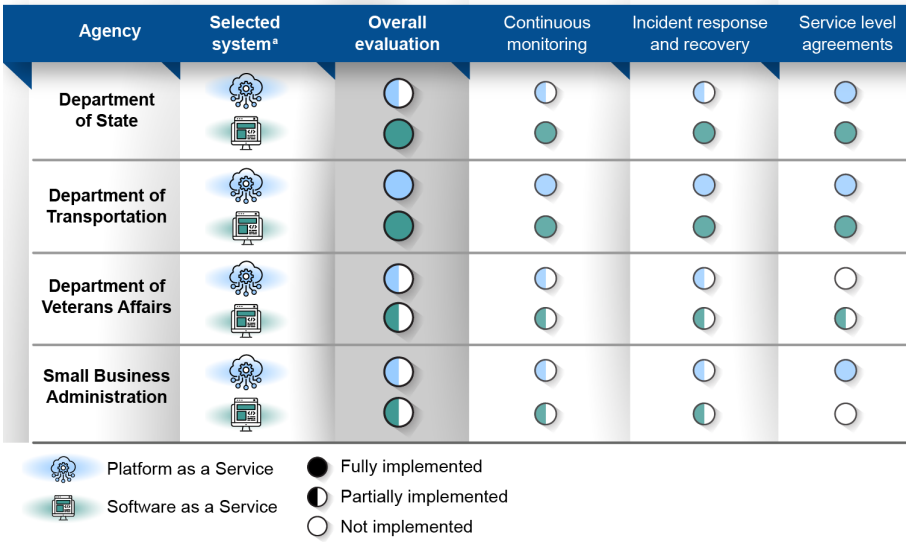
A report to congressional committees

For more information, contact: David B. Hinchman at HinchmanD@gao.gov

What GAO Found

Four selected agencies—the Departments of State, Transportation, Veterans Affairs (VA), and the Small Business Administration (SBA)—varied in their efforts to implement and ensure contractor compliance with three key cloud security practices. Specifically, one agency had fully implemented all three practices for two of its systems and one agency had fully implemented the practices for one of its systems. The agencies partially implemented the practices for the remaining five systems (see figure).

Agencies' Implementation of Key Cloud Security Practices



Sources: GAO analysis of agency documentation; Cetacons/stock.adobe.com (all icons); Agencies (logo). | GAO-26-108443

[a]Due to sensitivity concerns, GAO is not disclosing the names of the selected systems in this report. Systems are identified by their cloud service model.

For example, agencies fully performed continuous monitoring for three of the eight selected systems. Although most of the agencies developed and implemented a plan for continuous monitoring, they did not always review continuous monitoring deliverables from the provider. Agencies fully implemented the practice regarding service level agreements for five out of eight systems. For the remaining three systems, agencies' agreements did not consistently define performance metrics, including how they would be measured and the enforcement mechanisms.

Fully implementing the key practices will support the agencies' efforts to ensure the confidentiality, integrity, and availability of agency information in their cloud systems. For example, without a robust continuous monitoring program, the agencies may have diminished ability to identify and mitigate control deficiencies and emerging threats. Additionally, the agencies may not promptly detect unauthorized access attempts or anomalous activity, leaving critical systems and data exposed to compromise.

Why GAO Did This Study

Federal agencies are faced with the need to accelerate their adoption of cloud services while ensuring the systems that support their missions are secure. Consequently, working with cloud service providers to effectively implement information security controls is a vital part of reducing risks to agency systems.

The Federal Information Security Modernization Act of 2014 includes a provision for GAO to periodically evaluate federal agencies' information security policies and practices. This report assesses the extent to which selected agencies are ensuring contractor compliance with key cloud computing security practices.

To do so, GAO selected four agencies (State, Transportation, VA, SBA) based on their number of cloud authorizations, excluding agencies profiled in recent GAO reports. GAO reviewed two cloud systems at each agency, each of which represented a range of services. GAO administered a standard set of questions, compared documentation on the implementation of key cloud-related practices for each system identified in federal policies and guidance, and interviewed agency officials. GAO rated each agency as having fully, partially, or not implemented each practice for the selected systems.

What GAO Recommends

GAO is making 12 recommendations to State, VA, and the SBA to fully implement key cloud security practices. VA agreed with the recommendations, and State neither agreed nor disagreed. SBA did not provide comments on the report. State and VA also described actions taken or planned to address the recommendations.

Contents

Tables

Figures

Abbreviations

CISA	Cybersecurity and Infrastructure Security Agency
FedRAMP	Federal Risk and Authorization Management Program
FISMA	The Federal Information Security Modernization Act of 2014
GSA	General Services Administration
IT	information technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PaaS	platform as a service
SaaS	software as a service
SBA	Small Business Administration
SLA	service level agreement
VA	Department of Veterans Affairs

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

June 25, 2026

The Honorable Rand Paul, M.D.
Chairman
The Honorable Gary C. Peters
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable James Comer
Chairman
The Honorable Robert Garcia
Ranking Member
Committee on Oversight and Government Reform
House of Representatives

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.[1] Cloud services offer federal agencies a means to buy services more quickly and possibly at a lower cost than building, operating, and maintaining these computing resources themselves. As part of a comprehensive effort to transform information technology (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.[2]

However, as we have previously reported, the use of cloud computing also poses cybersecurity risks.[3] These risks arise when agencies and cloud service providers (providers) do not effectively implement security controls over their cloud services. Weaknesses in these controls could

[1]National Institute of Standards and Technology, *The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology*, Special Publication 800-145 (Gaithersburg, MD: September 2011).

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

[3]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).

lead to vulnerabilities affecting the confidentiality, integrity, and availability of agency information.

The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies to develop, document, and implement information security programs to protect the information and systems that support the agencies' operations and assets.[4] The act includes a provision for GAO to periodically evaluate federal agencies' information security policies and practices required by FISMA.[5]

Our objective for this review was to determine the extent to which selected agencies are ensuring contractor compliance with key cloud computing security practices. To address the objective, we identified a non-generalizable sample of four Chief Financial Officers Act agencies based[6] on the number of cloud authorizations issued, excluding agencies selected in recent GAO reports. Using the median number of authorizations, we randomly selected agencies with two at or above, and two below the median: Departments of State, Transportation, Veterans Affairs (VA), and the Small Business Administration (SBA).

We then administered a standard set of questions to the four agencies on their implementation of key cloud-related security practices for selected systems. Each agency was asked to provide documentation related to the implementation of the cloud security practices for two of its cloud

[4]The Federal Information Security Modernization Act of 2014 (FISMA 2014), Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014), largely superseded the Federal Information Security Management Act of 2002 (FISMA 2002), Title III of Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this report, FISMA refers both to FISMA 2014 and those provisions of FISMA 2002 that were either incorporated into FISMA 2014 or were unchanged and continue in full force and effect.

[5]44 U.S.C. § 3555(h)

[6]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)).

systems, each that represented a range of services.[7] 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 laws and guidance, including FISMA and publications from the Federal Risk and Authorization Management Program (FedRAMP), OMB, and the National Institute of Standards and Technology (NIST). From our review of the relevant guidance, we selected three key practices that agencies should apply to ensure effective provider protections of agency systems and data in a cloud environment, as well as associated evaluation criteria for each practice. The three key cloud security practices are continuous monitoring, incident response and recovery, and service level agreement implementation. We then obtained documentation from each agency, including contracts, incident response plans, and continuous monitoring plans. We analyzed these documents to determine whether the agency had implemented the three key practices for each of the agency's selected cloud systems. For each system, we assessed each agency's implementation of our evaluation criteria within each key practice area as follows:

- **Fully implemented**: the agency provided evidence which showed that it fully 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 or provided evidence insufficient to demonstrate implementation of any criteria.

To determine an overall rating for each system within each of the three key practice areas, we 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.

[7]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.

- **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 all 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 I includes additional information on our objective, scope, and methodology.

We conducted this performance audit from April 2025 to June 2026 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Background

Federal agencies increasingly use cloud computing to perform their missions. Cloud services provide benefits, including on-demand access to shared resources such as networks, servers, and data storage, and can enable agencies to deliver IT services more efficiently. Additionally, cloud services can provide agencies with opportunities to obtain IT capabilities more quickly and potentially at a lower cost than building and maintaining their own computing infrastructure. In pursuing these benefits, agencies may also encounter various risks and challenges, such as managing shared cybersecurity responsibilities with the provider.

Federal Legislation and Guidance on Cloud Service Cybersecurity

Federal legislation and guidance, such as FISMA and OMB's FedRAMP memoranda, specify requirements for federal agencies to protect systems and data, including systems used or operated by a contractor on behalf of a federal agency.

FISMA

FISMA is intended to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets, as well as the effective oversight of information security risks. FISMA requires each agency to develop, document, and implement an agency-wide information security program to provide risk-based protections for the information and information systems that support the operations and assets of the

agency, including those provided or managed by another entity on behalf of the agency.[8]

FedRAMP

OMB established FedRAMP in 2011 to facilitate the adoption and use of cloud services.[9] The program is intended to provide a standardized approach for selecting and authorizing the use of cloud services—referred to as cloud service offerings—that meet federal security requirements. Now managed by the General Services Administration (GSA), the program aims to ensure that cloud services have adequate information security, while also eliminating duplicative efforts and reducing operational costs.

In 2019, OMB updated the federal cloud computing strategy, now known as the Cloud Smart strategy, to provide agencies with guidance for acquiring secure and cost-effective cloud services.[10] The strategy established key requirements for agencies related to procuring cloud services and emphasized the importance of addressing security, procurement, and workforce considerations when adopting cloud computing. In implementing Cloud Smart, agencies are expected to address these requirements, including oversight by agency chief information officers, performing continuous monitoring of agencies' cloud systems, and the use of service level agreements that define the levels of service and performance expected from providers.

Subsequently, in December 2022, Congress enacted the FedRAMP Authorization Act as part of the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, which codified the FedRAMP program.[11] The act required OMB to, among other things, issue guidance defining the scope of FedRAMP and establish requirements for agencies to use it.[12]

[8]44 U.S.C. § 3554.

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

[10]Office of Management and Budget, *Federal Cloud Computing Strategy* (June 24, 2019), which superseded OMB's 2011 guidance of the same name, previously known as Cloud First.

[11]*James M. Inhofe National Defense Authorization Act for Fiscal Year 2023*, Pub. L. No. 117-263, div. E, title LIX, subtitle C, § 5921, 136 Stat. 2395, 3449, (December 23, 2022), codified at 44 U.S.C. § 3607 *et. seq*.

[12]44 U.S.C. § 3614.

In accordance with the act, in July 2024, OMB issued its *Modernizing the Federal Risk and Authorization Management Program (FedRAMP)* guidance.[13] The guidance defined the scope of FedRAMP, established requirements for the use of the program by federal agencies, and delineated responsibilities of the FedRAMP Board[14] and the program management office at the GSA.

OMB's M-24-15 guidance directs agencies to use FedRAMP when conducting risk assessments, security authorizations, and granting authority to operate for cloud services. Agencies are also directed to ensure that contracts require providers to comply with FedRAMP security authorization requirements and establish plans for responding to security and privacy incidents involving cloud services. In addition, FedRAMP requires providers to implement a continuous monitoring program that includes providing security deliverables, such as vulnerability scanning results, to agencies using their services.

Modernization of FedRAMP through the FedRAMP 20x Initiative

In March 2025, GSA announced FedRAMP 20x, a new modernization initiative aimed at improving the efficiency, speed, and security outcomes of FedRAMP. According to GSA, the 20x initiative seeks to reduce authorization timelines by up to 50 percent through process automation, improved stakeholder engagement, and enhanced reuse of security packages. Key components of the initiative are to require cloud services to automate the persistent production of security metrics to enable automated review, expand the FedRAMP Marketplace to improve transparency, and implement cloud-specific continuous monitoring best practices to strengthen cybersecurity posture. According to GSA and FedRAMP Program Management Office officials, FedRAMP 20x is designed to address longstanding stakeholder concerns around complexity, cost, and timeline predictability in the authorization process.

[13]Office of Management and Budget, *Modernizing the Federal Risk and Authorization Management Program (FedRAMP),* M-24-15 (Washington, D.C.: July 25, 2024).

[14]The FedRAMP Authorization Act, which was enacted in December 2022, established the FedRAMP Board, which is made up of officials from the Departments of Defense and Homeland Security, GSA, and other agencies that are appointed by OMB. The board is responsible for, among other things, serving as a resource for best practices to accelerate the process for obtaining a FedRAMP authorization, and establishing and regularly updating requirements and guidelines for security authorizations of cloud computing products and services.

According to GSA's publicly available timeline,[15]

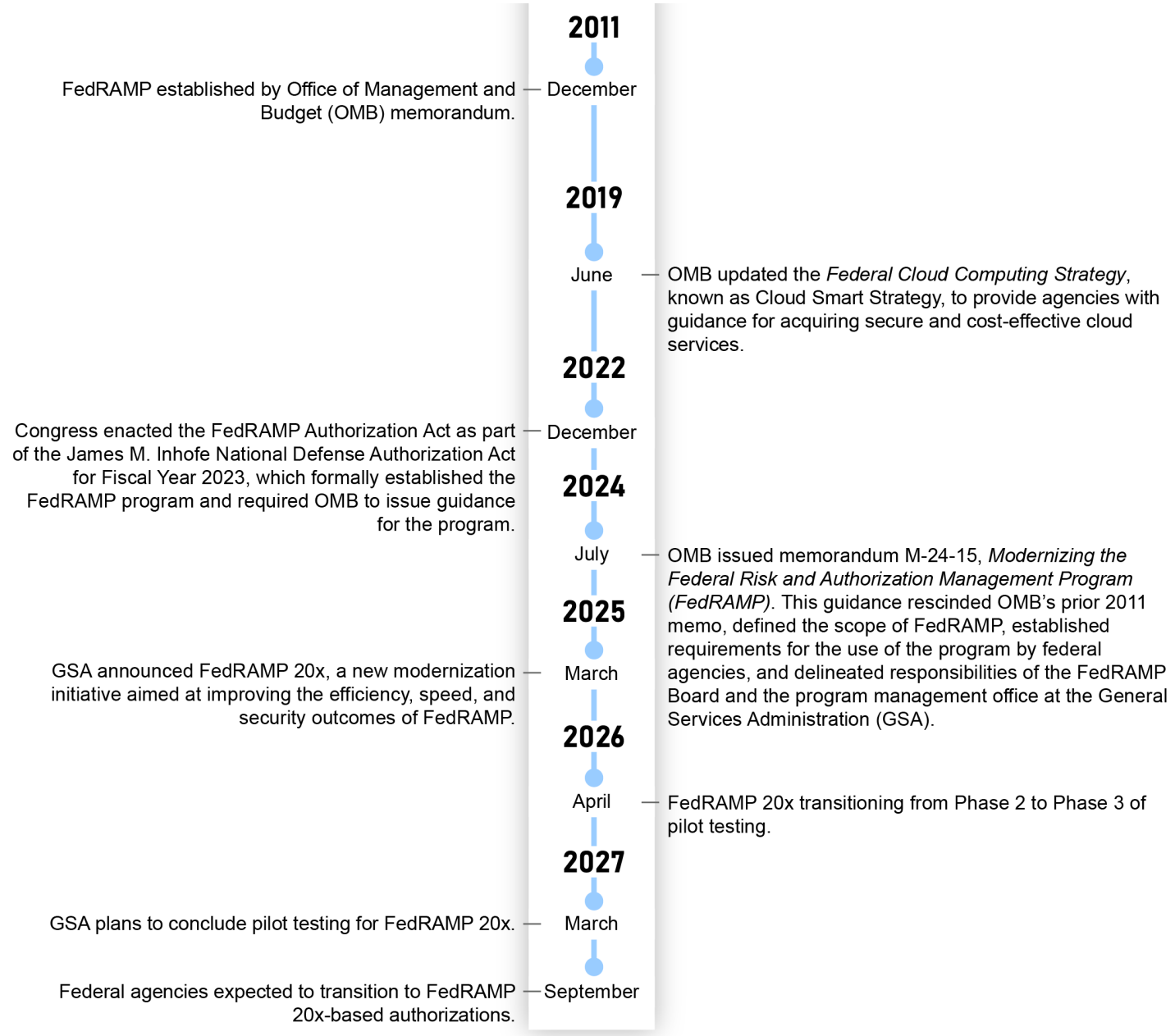
- Phase One, which included an initial 12 FedRAMP 20x Low pilot authorizations,[16] was completed in September 2025.
- Phase 2, which is currently ongoing, is a pilot for authorizing Moderate impact cloud systems and is expected to be completed by the second quarter of fiscal year 2026.
- Phase 3 will formalize all 20x Low and Moderate requirements for cloud service providers based on the outcome from the Phase 1 and Phase 2 pilots. This phase is expected to begin by the third quarter of fiscal year 2026 and completed by the fourth quarter of fiscal year 2026.
- Phase 4 will continue with wide-scale adoption of 20x Low and Moderate while piloting a path for 20x High authorizations. All previously authorized providers will be required to transition to machine-readable authorization data for both initial and continuing authorization. This phase is expected to begin by the first quarter of fiscal year 2027 and completed by the second quarter of fiscal year 2027.

FedRAMP 20x is expected to conclude all pilot testing by March 2027. Agencies will then be expected to transition to 20x-based authorizations by September 2027. See figure 1 for a timeline of guidance and future plans for FedRAMP.

[15]"Phased Delivery of FedRAMP 20x," FedRAMP 20x Overview, General Services Administration, accessed April 9, 2026, https://www.fedramp.gov/20x/.

[16]According to NIST's publication FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, there are three impact levels for systems. Low impact systems are most appropriate where the loss of confidentiality, integrity, and availability would result in limited adverse effects on an agency's operations, assets, or individuals. Moderate impact systems are most appropriate where the loss of confidentiality, integrity, and availability would result in serious adverse effects on an agency's operations, assets, or individuals. Serious adverse effects could include significant operational damage to agency assets, financial loss, or individual harm that is not loss of life or physical. High impact systems are usually related to law enforcement and emergency services systems, financial systems, health systems, and any other system where loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Figure 1: Timeline of Guidance and Future Plans for the Federal Risk and Authorization Management Program (FedRAMP) as of April 2026



Source: GAO analysis of federal law and guidance. | GAO-26-108443

Agencies Can Select from Various Cloud Service Models

Federal agencies can select different cloud models, which can comprise one or more cloud services, to support their missions and operations. 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. Each type of cloud service offers unique features and security implications that agencies should consider when implementing their cloud systems. NIST has identified three primary cloud service models.[17] These include:

- **Platform as a Service (PaaS)** includes platforms for developing, testing, and deploying software such as applications or information dashboards. The provider 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)** includes applications such as billing, email and office productivity, human resources functions, and document management. The provider delivers one or more applications and all the resources (operating system and programming tools) and underlying infrastructure, which the agency can use on demand.
- **Infrastructure as a Service** includes infrastructure for functions such as data storage, computing power, and backup and recovery services. The provider delivers and manages the basic computing infrastructure of servers, software, storage, and network equipment. The agency manages the operating system, programming tools and services, and applications.

Guidance on Key Cloud Security Practices

Federal guidance identifies several key practices that agencies should implement to help ensure the security of systems that rely on cloud services.[18] These practices include implementing continuous monitoring, establishing incident response and recovery capabilities, and defining service level agreements (SLA) that specify expected performance and security requirements. Additionally, in March 2026, the Council of the Inspectors General on Integrity and Efficiency published Best Practices

[17]National Institute of Standards and Technology, *Special Publication 800-145* and *Cloud Computing Reference Architecture*, Special Publication 500-292 (Sept. 2011).

[18]For example, National Institute of Standards and Technology, *Guidelines on Security and Privacy in Public Cloud Computing*, SP 800-144, (Dec. 2011), *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, SP 800-37, Rev. 2 (Dec. 2018), and *Security and Privacy Controls for Information Systems and Organizations,* SP 800-53, Rev. 5 (Sept. 2020).

for Federal Agencies to Strengthen Cloud Security.[19] The report identified common best practices for implementing effective cloud security, to include implementing effective continuous monitoring controls and providing oversight of providers. The practices were based on findings identified in 35 reports issued by 19 Offices of Inspectors General and GAO between 2014 and 2024. The following is a description of the three key cloud security practices.

Continuous monitoring. Continuous monitoring is a process of ongoing awareness of information security, threats and vulnerabilities to facilitate risk-based decision making. It involves maintaining ongoing awareness of security controls and system vulnerabilities through automated tools, vulnerability scanning, configuration assessments, and log monitoring. FedRAMP requires providers to regularly report security status information to agencies to support this process. Without continuous monitoring, decision makers may have limited to no assurance that controls are in place and working, and an increased risk that vulnerabilities are not identified in a timely manner.

Incident response and recovery. Providers and agencies must document procedures for responding to and recovering from security and privacy incidents for the cloud system. These procedures help agencies ensure that they are able to quickly respond to and recover from incidents, and that information resources are protected.

Service level agreements. SLAs are agreements that set requirements for the selected providers, such as performance and security expectations. These agreements often include requirements related to system availability, security responsibilities, incident response timelines, and data protection requirements. SLAs define the level of service and performance expected from a provider, how that performance will be measured, and what enforcement mechanisms will be used to ensure the specified performance levels are achieved. Such agreements may also specify security requirements and reporting procedures to help agencies ensure that cloud services are performed effectively, efficiently, and securely.

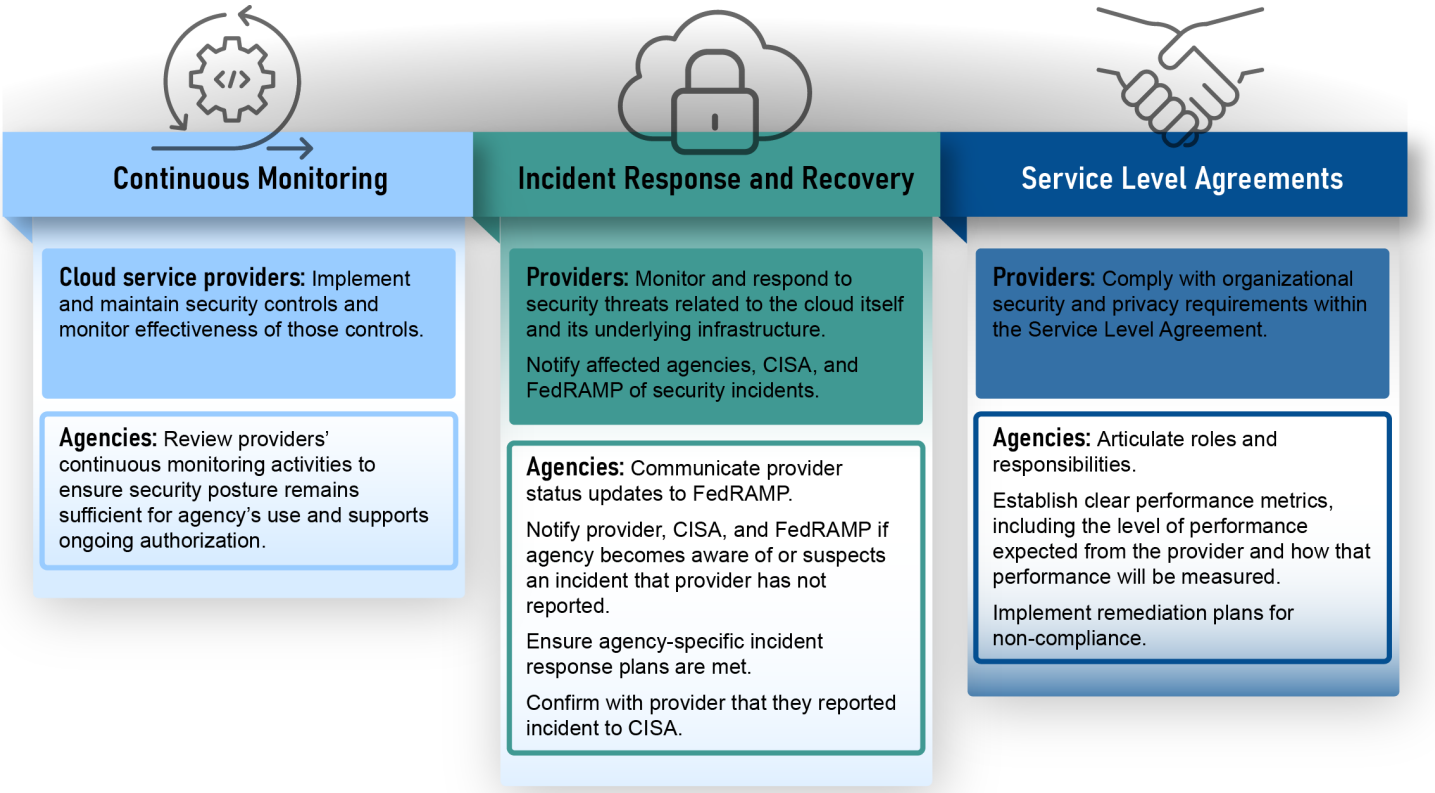
[19]Council of the Inspectors General on Integrity and Efficiency, *Best Practices for Federal Agencies to Strengthen Cloud Security* (March 2026), https://www.ignet.gov/sites/default/files/files/Best-Practices-for-Federal-Agencies-to-Strengthen-Cloud-Security.pdf.

Agencies and Providers Share Cybersecurity Responsibilities

Federal agencies typically rely on providers to provide and manage cloud infrastructure and services. As such, the implementation of effective information security controls becomes more important. The effective implementation of a standardized process for securing cloud environments could reduce risks to agency systems and information maintained on an agency's behalf (by a provider). Under federal guidance and leading cybersecurity practices, security responsibilities are often shared between the agency and the provider.[20] Figure 2 demonstrates the shared responsibilities between agencies and providers related to the three key practices.

[20]FedRAMP, "Continuous Monitoring Overview", FedRAMP Documentation, accessed January 21, 2026, https://www.fedramp.gov/docs/rev5/playbook/csp/continuous-monitoring/overview/#cloud-service-provider-csp, and "Incident Communication", Rev5 Continuous Monitoring Playbook, accessed January 22, 2026, https://www.fedramp.gov/docs/rev5/playbook/csp/continuous-monitoring/incident-communication/; Office of Management and Budget, *Federal Cloud Computing Strategy* (June 24, 2019); and National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations,* SP 800-53, Rev. 5 (Sept. 2020).

Figure 2: Shared Responsibilities Between Agencies and Cloud Service Providers Within Key Cloud Security Practices



CISA = Cybersecurity and Infrastructure Security Agency, FedRAMP = Federal Risk and Authorization Management Program

Sources: GAO analysis of federal law and guidance; Cetacons/stock.adobe.com (icons). | GAO-26-108443

GAO Has Previously Reported on Agencies' Efforts to Secure Cloud Systems

We have issued a series of reports over the past decade examining federal agencies' use of cloud computing, management of cloud security risks, and oversight of providers.

In September 2024, we assessed the 24 Chief Financial Officers Act agencies' cloud procurement guidance and alignment with OMB's Cloud Smart Strategy.[21] Among other things, we found that most agencies did not have guidance that ensured that all four elements of an adequate SLA

[21]GAO, *Cloud Computing: Agencies Need to Address Key OMB Procurement Requirements*, GAO-24-106137 (Washington, D.C.: Sept. 10, 2024).

were in place for vendor-deployed cloud services.[22] Specifically, 11 agencies did not have guidance that required SLAs with providers establish clear performance metrics, and 17 agencies did not have language requiring remediation plans for non-compliance. We made 17 recommendations to agencies to improve guidance for incorporating OMB's required elements for SLAs, including clear performance metrics and remediation plans for non-compliance. As of April 2026, 12 out of 17 of those recommendations have not been fully implemented.

In May 2023, we evaluated six key cloud security practices at four agencies and found that none of the agencies fully implemented all practices for the systems reviewed.[23] We identified gaps in areas such as continuous monitoring implementation, SLA security metrics and enforcement provisions, and documenting incident response and recovery procedures. We made 35 recommendations to, among other things, improve documentation of responsibilities, strengthen continuous monitoring, and ensure SLA security requirements are clearly defined. The Department of Homeland Security agreed with our recommendations, while Agriculture, Labor and Treasury neither agreed nor disagreed. As of April 2026, nine recommendations have not been fully implemented.

In April 2016, we identified 10 key practices that federal and private-sector guidance noted should be included in service level agreements when acquiring IT services through a provider.[24] Our review of five agencies' (Departments of Defense, Health and Human Services, Homeland Security, Treasury, and Veterans Affairs) cloud service contracts found that not all 10 key practices were included in these contracts. We recommended that OMB include all 10 key practices in future guidance to agencies and that Defense, Health and Human Services, Homeland Security, Treasury, and Veterans Affairs implement SLA guidance and incorporate applicable key practices into their SLAs. All the agencies have implemented the recommendations.

[22]The four elements are continuous awareness of the confidentiality, integrity, and availability of its information, granularly articulated roles and responsibilities, clear performance metrics, and remediation plans for non-compliance.

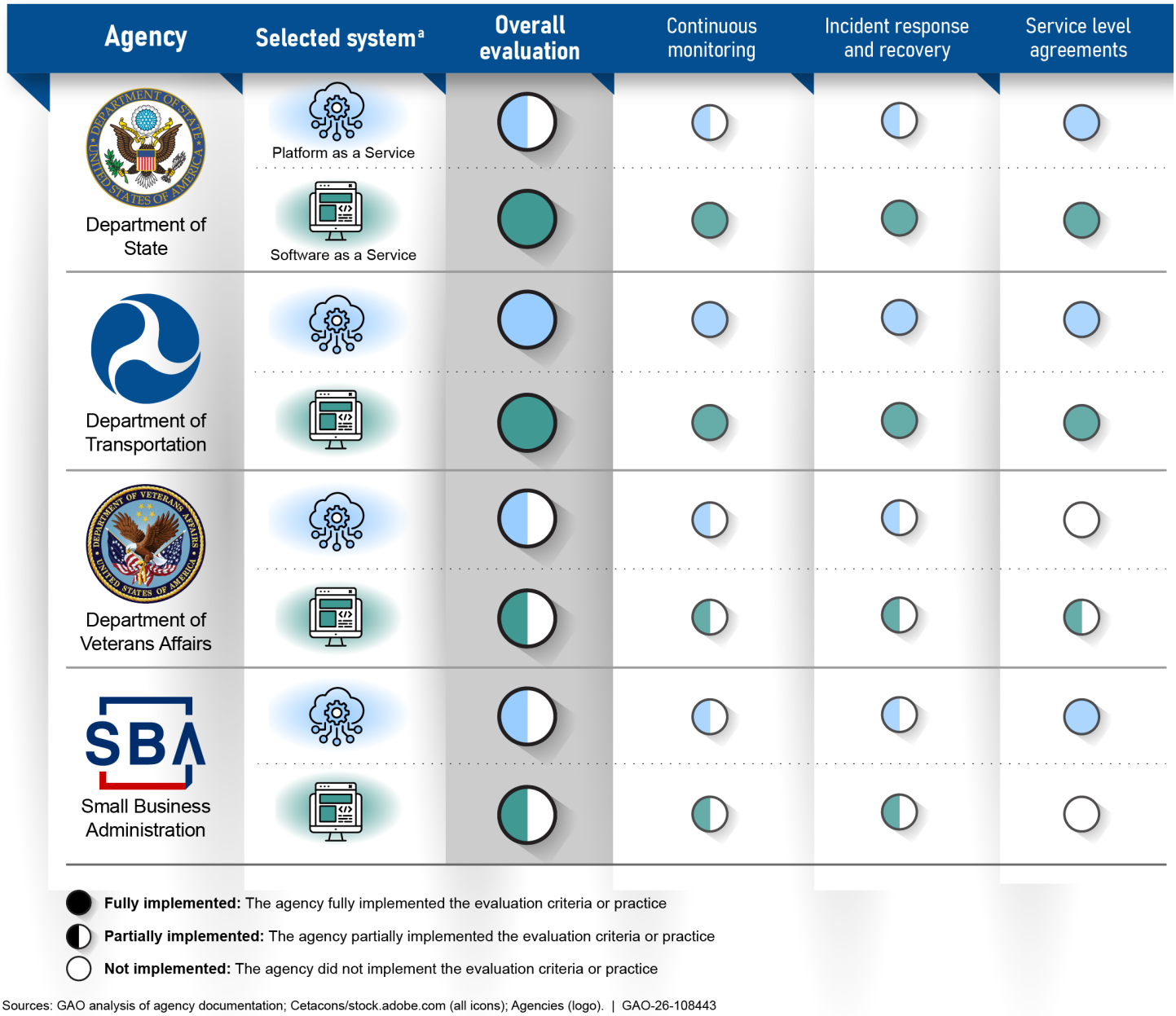
[23]GAO, *Cloud Security: Selected Agencies Need to Fully Implement Key Practices*, GAO-23-105482 (Washington, D.C.: May 18, 2023).

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

Selected Agencies Have Not Fully Implemented Key Cloud Security Practices

The four selected agencies—the Departments of State, Transportation, and VA, as well as the SBA–varied in their efforts to implement the key cloud security practices for ensuring effective provider protections of agency systems and data (see appendix I for the evaluation criteria associated with the key cloud security practices). Specifically, one of the four selected agencies (Transportation) had fully implemented all three practices for both of its selected systems, and one agency (State) had fully implemented the practices for one of its selected systems. The remaining agencies had partially implemented the key practices for the remaining five cloud systems (see figure 3). Ensuring implementation of these key practices is important in cloud computing environments, especially given the sensitive nature of federal data and the increasing reliance on third-party providers to host and manage information. 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. The implementation of each practice is discussed in greater detail below.

Figure 3: Summary of Selected Agencies' Implementation of Key Cloud Security Practices



Sources: GAO analysis of agency documentation; Cetacons/stock.adobe.com (all icons); Agencies (logo). | GAO-26-108443

[a]Due to sensitivity concerns, we are not disclosing the names of the selected systems in this report. Systems are identified by their cloud service model.

Agencies Did Not Fully Implement Continuous Monitoring for Their Selected Systems

According to federal guidance, agencies are to perform continuous monitoring of their cloud systems.[25] 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 provider. 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.

As shown in table 1, agencies fully performed continuous monitoring for three of the eight selected systems and partially performed continuous monitoring for the five remaining systems.

[25]FedRAMP, "Continuous Monitoring Overview," FedRAMP Documentation, accessed January 21, 2026, https://www.fedramp.gov/docs/rev5/playbook/csp/continuous-monitoring/overview/#cloud-service-provider-csp; National Institute of Standards and Technology, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, SP 800-37, Rev. 2 (Dec. 2018), *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, SP 800-137 (Sep. 2011) and *Security and Privacy Controls for Information Systems and Organizations,* SP 800-53, Rev. 5 (Sept. 2020); Office of Management and Budget, *Modernizing the Federal Risk and Authorization Management Program (FedRAMP),* M-24-15 (Washington, D.C.: July 25, 2024), and *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, M-21-31 (Washington, D.C.: August 27, 2021).

Table 1: Agency Implementation of Continuous Monitoring Practices

Agency	Selected system	Developed and implemented continuous monitoring plan	Reviewed continuous monitoring deliverables from the cloud service provider	Documented use of vulnerability management tools	Collected and reviewed audit logs	Overall evaluation
Department of State	PaaS	●	○	●	●	◐
	SaaS	●	●	●	●	●
Department of Transportation	PaaS	●	●	●	●	●
	SaaS	●	●	●	●	●
Department of Veterans Affairs	PaaS	●	●	●	○	◐
	SaaS	●	●	●	○	◐
Small Business Administration	PaaS	◐	○	◐	○	◐
	SaaS	●	●	◐	●	◐

PaaS = Platform as a Service; SaaS = Software as a Service

● Fully implemented: The agency fully implemented the evaluation criteria or practice.

◐ Partially implemented: The agency partially implemented the evaluation criteria or practice.

○ Not implemented: The agency did not implement the evaluation criteria or practice.

Source: GAO analysis of agency documentation. | GAO-26-108443

One agency—Transportation—fully implemented the practice for both of its systems. One agency—State—fully implemented the practice for one of its systems and partially implemented the practice for its other system. The other two agencies (VA and SBA) partially implemented the practice for each of their two systems.

Transportation developed a plan for continuously monitoring the security controls that are the agency's responsibility for both of its systems. It also reviewed continuous monitoring deliverables from the provider, documented the use of vulnerability management tools, and provided evidence that it collected and reviewed audit logs for both of its systems.

State developed and implemented a plan for continuously monitoring the security controls that are the agency's responsibility, documented the use of vulnerability management tools, and provided evidence that it collected and reviewed audit logs for each of its systems. However, while State provided evidence that it had reviewed continuous monitoring deliverables from the provider of its SaaS system, it did not demonstrate reviews for its PaaS system. According to agency officials, State does not have monthly continuous monitoring meetings with the PaaS provider that

includes the typical review of certain deliverables. Agency officials stated the system is included in a department continuous assessment program and that they would provide additional information. However, State did not provide additional information and noted that the responsible cyber teams had moved within the agency as part of a reorganization.

VA developed a plan for continuously monitoring the security controls that are the agency's responsibility, reviewed continuous monitoring deliverables from the provider, and documented the use of vulnerability management tools for each of its systems. The agency also documented policies and procedures for audit log management for both the PaaS and SaaS systems; however, it did not provide evidence it collected or reviewed audit logs from the provider. According to VA's Cybersecurity Program Directive, the collection of audit logs from all cloud systems is mandated. In written statements, VA officials stated that the agency conducts monthly reviews following the FedRAMP guideline for continuous monitoring. However, they did not provide evidence that they collect and review audit logs. VA officials noted that the agency is in the beginning stages of migrating the applications to a new monitoring system.

SBA developed a plan for continuously monitoring the security controls that are the agency's responsibility for both systems. However, the agency did not demonstrate implementation of the continuous monitoring plan for the PaaS system. In addition, while SBA reviewed continuous monitoring deliverables and collected and reviewed audit logs for its SaaS system, it had not done so for its PaaS system. Further, although SBA documented vulnerability management plans for both systems, it did not provide evidence of the use of vulnerability management tools for either of the systems, such as a report from a vulnerability scanning tool. Additionally, the PaaS system security plan was not signed. SBA officials stated that they would provide a signed plan but did not do so.

While most of the selected agencies stated that they believed they were continuously monitoring their systems' security controls, they did not provide evidence of fully doing so. Without a robust continuous monitoring program for its cloud systems, the selected agencies may have diminished ability to identify and mitigate control deficiencies and emerging threats. Additionally, the agencies may not promptly detect unauthorized access attempts or anomalous activity, leaving critical systems and data exposed to compromise.

Three of Four Agencies Did Not Fully Document Incident Response and Recovery Procedures for Their Selected Systems

According to federal guidance, agencies are to document procedures for responding to and recovering from security and privacy incidents for the cloud system.[26] For example, guidance from FedRAMP includes requirements that agencies, providers, and the Cybersecurity and Infrastructure Security Agency (CISA) coordinate incident response and recovery. These procedures help ensure that agencies can quickly respond to and recover from incidents, and that information resources are protected.

As shown in table 2, agencies fully implemented incident response practices for three of the eight systems and partially implemented incident response practices for the five remaining systems.

[26]FedRAMP, "Incident Communication," Rev5 Continuous Monitoring Playbook, accessed January 22, 2026, https://www.fedramp.gov/docs/rev5/playbook/csp/continuous-monitoring/incident-communication/; National Institute of Standards and Technology, *Guidelines on Security and Privacy in Public Cloud Computing*, SP 800-144 (Dec. 2011) and *Security and Privacy Controls for Information Systems and Organizations*, SP 800-53, Rev. 5 (Sept. 2020); Office of Management and Budget, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements*, M-25-04 (Washington, D.C.: January 15, 2025), *FY 2025 CIO FISMA Metrics*, version 1.1 (December 2024), and *Federal Cloud Computing Strategy* (June 24, 2019).

Table 2: Agency Documented Procedures for Responding to and Recovering from Security and Privacy Incidents for the Cloud System

Agency	Selected system	Agency had plans or procedures for identifying, containing, and mitigating cloud security incidents	Agency had plans or procedures for coordinating with cloud service provider and the Cybersecurity and Infrastructure Security Agency	Agency had plans or procedures for ensuring providers report security incidents promptly	Agency had plans or procedures for measuring and tracking incident response time	Agency had plans or procedures for testing incident response and recovery procedures	Overall evaluation
Department of State	PaaS	●	◐	●	●	●	◐
	SaaS	●	●	●	●	●	●
Department of Transportation	PaaS	●	●	●	●	●	●
	SaaS	●	●	●	●	●	●
Department of Veterans Affairs	PaaS	●	●	●	○	●	◐
	SaaS	●	●	●	●	○	◐
Small Business Administration	PaaS	◐	◐	○	◐	◐	◐
	SaaS	◐	◐	●	◐	●	◐

PaaS = Platform as a Service; SaaS = Software as a Service

● Fully implemented: The agency fully implemented the evaluation criteria or practice.

◐ Partially implemented: The agency partially implemented the evaluation criteria or practice.

○ Not implemented: The agency did not implement the evaluation criteria or practice.

Source: GAO analysis of agency documentation. | GAO-26-108443

One agency (Transportation) fully implemented the incident response practice for both of its selected systems. Another agency (State) fully implemented the practice for one of its systems and partially implemented the practice for its other system. The remaining two agencies (VA and SBA) partially implemented the practice for each of their two systems.

Specifically, Transportation developed plans and procedures for identifying, containing, and mitigating cloud security incidents; coordinating with providers and CISA; ensuring providers report incidents promptly; measuring and tracking incident response time; and testing incident response and recovery procedures for both of its systems.

State developed plans and procedures for identifying, containing, and mitigating cloud security incidents; coordinating with CISA; measuring and tracking incident response time; and testing incident response and

recovery procedures for both the systems. However, although the agency had incident response procedures for both the systems that required prompt incident reporting by providers, it did not have procedures for coordinating with providers for the PaaS system. State incident reporting requirements for PaaS systems referenced procedures documented in system plans but State did not provide those plans. Officials noted that the responsible cyber teams had moved within State as part of a reorganization.

VA developed plans and procedures for identifying, containing, and mitigating cloud security incidents; coordinating with the provider and CISA; and ensuring prompt incident reporting by providers for both the systems. However, although VA developed incident response plans and procedures for both systems, the agency did not have plans or procedures for measuring and tracking incident response time for its PaaS system.

Additionally, VA did not have plans or procedures for testing incident response and recovery procedures for its SaaS system. VA officials stated that the vendor conducted incident response testing in October 2025; however, evidence of that testing or testing procedures was not provided. VA officials further stated that both their SaaS and PaaS systems are externally owned and operated by the provider and that the provider's documentation and reporting could not be provided. The officials noted that the agency is in the beginning stages of migrating the applications to a new monitoring system.

SBA developed a plan for prompt incident reporting by providers for its SaaS system but did not do so for its PaaS system. SBA also provided an incident response plan that included procedures for identifying, containing, and mitigating cloud security incidents; coordinating with providers and CISA; and tracking incident response time for both systems. However, the plan was not signed. Additionally, while SBA developed plans or procedures for incident response testing requirements for both the systems, the plan for the PaaS system was not signed.

Without clearly defined and tested procedures for responding to cloud-specific security and privacy incidents, the selected agencies risk delayed detection, containment, and remediation of cyber events. Furthermore, the agency may not be able to ensure that recovery activities are effective. As we have previously reported, high-profile cyber incidents like the SolarWinds and Microsoft Exchange attacks underscore the threats

that federal agencies and service providers face in ensuring proper incident response and recovery.[27]

Half of the Agencies' Service Level Agreements Defined Performance Metrics for Both Selected Systems

According to federal guidance, agencies contracting with a provider are to have an SLA that defines performance metrics.[28] 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 provider should define: (1) performance metrics; (2) how the performance will be measured; and (3) enforcement mechanisms to ensure the provider provides the specified performance levels.

As shown in table 3, the selected agencies had SLAs that fully defined performance metrics for five of the eight selected systems, partially defined for one, and did not define security metrics for the remaining two.

[27]Beginning in September 2019, a campaign of cyberattacks by a foreign threat actor breached the computing networks at SolarWinds—a network management software company widely used in the federal government to monitor network activity on federal systems. GAO, *Cybersecurity: Federal Response to SolarWinds and Microsoft Exchange Incidents,* GAO-22-104746 (Washington, D.C.: Jan. 13, 2022).

[28]Office of Management and Budget, *Federal Cloud Computing Strategy* (June 24, 2019).

Table 3: Agency Implementation of a Service Level Agreement (SLA) with Cloud Service Provider That Defined Performance Metrics

Agency	Selected system	SLA defined performance metrics	SLA defined how the performance would be measured	SLA defined the enforcement mechanisms	Overall evaluation
Department of State	PaaS	●	●	●	●
	SaaS	●	●	●	●
Department of Transportation	PaaS	●	●	●	●
	SaaS	●	●	●	●
Department of Veterans Affairs	PaaS	○	○	○	○
	SaaS	●	○	○	◐
Small Business Administration	PaaS	●	●	●	●
	SaaS	○	○	○	○

PaaS = Platform as a Service; SaaS = Software as a Service

● Fully implemented: The agency fully implemented the evaluation criteria or practice.

◐ Partially implemented: The agency partially implemented the evaluation criteria or practice.

○ Not implemented: The agency did not implement the evaluation criteria or practice.

Source: GAO analysis of agency documentation. | GAO-26-108443

Two agencies—State and Transportation—fully implemented the practice for both their selected systems. VA partially implemented the practice for one system and did not implement the practice for its other system. Another agency—SBA—fully implemented the practice for one of its selected systems but did not implement the practice for its other system.

Specifically, State and Transportation had SLAs for both of their systems that defined performance metrics. Additionally, both agencies' SLAs defined how performance would be measured and enforcement mechanisms to ensure their providers met agreed upon performance levels.

VA had a contract with defined performance metrics for its SaaS system; however, the agreement did not define how the performance would be measured or include enforcement mechanisms. For the selected PaaS system, VA pointed to websites with generalized SLA language, but none of these documents demonstrated an SLA between the agency and the provider that included performance metrics, measures or enforcement mechanisms.

While SBA had an SLA for its PaaS system that defined performance metrics, how performance would be measured, and included enforcement

mechanisms, it did not have one for its SaaS system. Agency officials stated that SBA is in the process of transitioning to an enterprise SLA for its technology services and noted that the estimated timeline for implementation was nine months.

Until the agencies ensure that their cloud systems have SLAs that measure and enforce performance, they may not receive the services they require. Additionally, agencies risk being unable to hold providers accountable for meeting contracted performance levels and may not have recourse if service levels fall below expectations. Consequently, federal agencies face the prospects of not fulfilling their mission, wasting appropriated funds, and a lack of accountability that shifts risks from the provider further onto the government.

Conclusions

Federal agencies are faced with the need to accelerate their adoption of cloud services while ensuring the systems that support their missions are safe and secure when operating in the cloud. But agencies must also effectively implement cloud security and ensure the protection of agency data maintained in the cloud. Purchasing IT services through a cloud service provider can enable agencies to avoid paying the full cost for the resources that would typically be needed on premises to provide such services. Consequently, working with cloud service providers to effectively implement information security controls is a vital part of reducing risks to agency systems.

The four selected agencies—State, Transportation, VA, and SBA—varied in their efforts to implement and ensure contractor compliance with the key cloud security practices. In particular, three of the four selected agencies had one or more systems with shortfalls in implementing continuous monitoring, documenting incident response and recovery procedures, and properly defining service level agreements.

Going forward, it will be important for the selected agencies to ensure implementation of the key cloud security practices to address a number of increased risks. For example, until key practices associated with continuous monitoring are fully implemented, the agencies may not promptly detect unauthorized access attempts or anomalous activity, leaving critical systems and data exposed to compromise. Without clearly defined and tested incident response and recovery procedures, the selected agencies risk delayed detection, containment, and remediation of cyber events. Furthermore, the agency may not be able to ensure that recovery activities are effective. Additionally, without properly defined

SLAs, agencies may not receive the services they require or be able to hold providers accountable if service levels fall below expectations.

Recommendations for Executive Action

We are making a total of 12 recommendations: two to State, five to VA, and five to SBA.

The Secretary of State should ensure that the agency fully implements continuous monitoring for its selected PaaS system, to include reviewing continuous monitoring deliverables from the cloud service provider. (Recommendation 1)

The Secretary of State should ensure that the agency fully implements incident response and recovery for its selected PaaS system, to include documenting plans or procedures for coordinating incident response and recovery with providers. (Recommendation 2)

The Secretary of Veterans Affairs should ensure that the agency fully implements continuous monitoring for its selected PaaS system, to include collecting and reviewing audit logs. (Recommendation 3)

The Secretary of Veterans Affairs should ensure that the agency fully implements continuous monitoring for its selected SaaS system, to include collecting and reviewing audit logs. (Recommendation 4)

The Secretary of Veterans Affairs should ensure that the agency fully implements incident response and recovery for its selected PaaS system, to include documenting plans or procedures for measuring and tracking incident response time. (Recommendation 5)

The Secretary of Veterans Affairs should ensure that the agency fully implements incident response and recovery for its selected SaaS system, to include documenting plans or procedures for testing incident response and recovery procedures. (Recommendation 6)

The Secretary of Veterans Affairs should ensure that the agency's service level agreements with providers define performance metrics, including how they are measured and the enforcement mechanisms. (Recommendation 7)

The Administrator of the Small Business Administration should ensure that the agency fully implements continuous monitoring for its selected PaaS system, to include implementing a continuous monitoring plan, reviewing continuous monitoring deliverables from the cloud service

provider, documenting the use of vulnerability management tools, and collecting and reviewing audit logs. (Recommendation 8)

The Administrator of the Small Business Administration should ensure that the agency fully implements continuous monitoring for its selected SaaS system, to include documenting the use of vulnerability management tools. (Recommendation 9)

The Administrator of the Small Business Administration should ensure that the agency fully implements incident response and recovery for its selected PaaS system, to include documenting plans or procedures for identifying, containing, and mitigating cloud security incidents; coordinating incident response and recovery with providers and the Cybersecurity and Infrastructure Security Agency; ensuring providers report incidents promptly; measuring and tracking incident response time; and testing incident response and recovery procedures. (Recommendation 10)

The Administrator of the Small Business Administration should ensure that the agency fully implements incident response and recovery for its selected SaaS system, to include documenting plans or procedures for identifying, containing, and mitigating cloud security incidents; coordinating incident response and recovery with providers and the Cybersecurity and Infrastructure Security Agency; and measuring and tracking incident response time. (Recommendation 11)

The Administrator of the Small Business Administration should ensure that the agency's service level agreements with providers define performance metrics, including how they are measured and the enforcement mechanisms. (Recommendation 12)

Agency Comments and Our Evaluation

We provided a draft of this report to the Departments of State, Transportation, and VA, GSA, and the SBA for their review and comment. We received responses from State, Transportation, and VA. GSA and the SBA did not provide comments on the report.

- In written comments, reprinted in appendix II, State neither agreed nor disagreed with our two recommendations. Specifically, for the first recommendation, State responded that it had developed formal procedures to fully implement continuous monitoring for the PaaS system and provided additional information on those procedures. Additionally, the department stated that it would assess and implement any necessary changes identified through this monitoring, based on system scope, the criticality of findings, and assigned responsibilities. However, while the procedures call for the review of deliverables, as we reported earlier, State did not provide evidence that it had performed these reviews for the PaaS system. Accordingly, we maintain that State should review continuous monitoring deliverables from the cloud provider. We will follow up with the agency to validate its implementation of the recommendation.

  State further noted that it had established draft procedures for incident response and recovery for the PaaS system to address the second recommendation and provided details about those procedures. Documenting plans or procedures for coordinating incident response and recovery with providers can help State reduce the risk of delayed detection, containment, and remediation of cyber events. Once the draft procedures are finalized, we plan to follow up with the agency to validate its implementation of the recommendation.

- In written comments, reprinted in appendix III, Transportation disagreed with a recommendation originally included in the draft of this report to ensure that the agency fully implements continuous monitoring for its selected SaaS system, to include documenting the use of vulnerability management tools. The agency provided additional documentation that it had not previously provided demonstrating that it used vulnerability management tools for the selected SaaS system. Upon our review of the documentation, we agreed that Transportation had sufficiently addressed the key practice for the selected cloud system. Accordingly, we removed this finding and withdrew the recommendation from the final report. Transportation also provided technical comments, which we have incorporated into the report, as appropriate.

- In written comments, reprinted in appendix IV, VA agreed with our five recommendations. The agency described actions that it plans to implement by November 2026 to address the recommendations. Specifically, regarding the two recommendations to fully implement continuous monitoring for its selected PaaS and SaaS systems, VA stated that it is deploying new monitoring solutions that are expected to enhance the agency's ability to continuously monitor the selected SaaS and PaaS systems, to include collecting and reviewing audit logs.

  VA further noted that the new monitoring system will also address our two recommendations for measuring and tracking incident response time for both its selected PaaS and SaaS systems. Specifically, VA stated that implementation of the monitoring solution will enhance VA's capability to document plans and procedures for measuring and tracking incident response time for both its selected PaaS and SaaS systems. In addition, VA stated that it will provide details on actions to address how VA measures service level agreement performance and utilizes enforcement mechanisms, as we recommended.

We are sending copies of this report to the appropriate congressional committees, the Secretaries and agency heads of the departments and agencies in this report, and other interested parties. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

If you or your staff have any questions about this report, please contact me at HinchmanD@gao.gov. Contact points for our Offices of Congressional Relations and Media Relations may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix V.

//SIGNED//

David B. Hinchman
Director, Information Technology and Cybersecurity

Appendix I: Objective, Scope, and Methodology

Our objective was to determine the extent to which selected agencies are ensuring contractor compliance with key cloud computing security practices.

To address our objective, we identified a nongeneralizable sample of four Chief Financial Officers Act agencies[1] that currently use cloud services. To select the agencies, we analyzed Federal Risk and Authorization Management Program (FedRAMP) marketplace data and totaled the reported number of FedRAMP cloud services for each agency. We then calculated the median number of services as 56, rounded to the nearest whole number. We organized the agencies into two groups: agencies with 56 or more services and agencies with fewer than 56 services. From these groups, we excluded agencies assessed in recent GAO reports.[2] We also excluded the Department of Education due to a proposed reorganization that would likely have significantly affected the timeframe and resources required for review. Randomly selecting two agencies from each group resulted in four agencies chosen for review—the Departments of State, Transportation, Veterans Affairs, and the Small Business Administration.

To identify key security practices for ensuring effective cloud service provider (provider) protections of agency systems and data in a cloud environment, we reviewed federal IT laws and guidance, including agency responsibilities under the Federal Information Security Modernization Act

[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 a prior report, we assessed the extent to which four agencies—the Department of Health and Human Services, the General Services Administration, the Environmental Protection Agency, and the U.S. Agency for International Development—had addressed key elements of the FedRAMP authorization process. 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). We also assessed the extent to which four agencies—the Departments of Agriculture, Homeland Security, Labor, and Treasury—implemented key cloud security practices. Thus, we excluded these eight agencies from review. GAO, *Cloud Security: Selected Agencies Need to Fully Implement Key Practices,* GAO-23-105482 (Washington, D.C.: May 18, 2023).

(FISMA) of 2014 (44 U.S.C. § 3554)[3] and publications from the Federal Risk and Authorization Management Program (FedRAMP),[4] the Office of Management and Budget (OMB)[5] and the National Institute of Standards and Technology (NIST).[6] We identified three key practices for information systems hosted in the cloud: continuous monitoring, incident response and recovery, and service level agreements. For each practice, we identified specific criteria for ensuring provider protections in a cloud environment that help agencies maintain robust security measures for their cloud systems (see table 4). We then developed a standard set of questions to address our objective.

[3]The Federal Information Security Modernization Act of 2014 (FISMA 2014), Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014), largely superseded the Federal Information Security Management Act of 2002 (FISMA 2002), Title III of Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this report, FISMA refers both to FISMA 2014 and those provisions of FISMA 2002 that were either incorporated into FISMA 2014 or were unchanged and continue in full force and effect.

[4]FedRAMP, "Continuous Monitoring Overview," FedRAMP Documentation, accessed January 21, 2026, https://www.fedramp.gov/docs/rev5/playbook/csp/continuous-monitoring/overview/#cloud-service-provider-csp, and "Incident Communication," Rev5 Continuous Monitoring Playbook, accessed January 22, 2026, https://www.fedramp.gov/docs/rev5/playbook/csp/continuous-monitoring/incident-communication/.

[5]Office of Management and Budget, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements*, M-25-04 (Washington, D.C.: January 15, 2025*), FY 2025 CIO FISMA Metrics*, version 1.1 (December 2024), *Modernizing the Federal Risk and Authorization Management Program (FedRAMP),* M-24-15 (Washington, D.C.: July 25, 2024), *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, M-21-31 (Washington, D.C.: August 27, 2021), and *Federal Cloud Computing Strategy* (June 24, 2019).

[6]National Institute of Standards and Technology, *Guidelines on Security and Privacy in Public Cloud Computing*, SP 800-144, (Dec. 2011), *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, SP 800-37, Rev. 2 (Dec. 2018), *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations,* SP 800-137 (Sep. 2011) and *Security and Privacy Controls for Information Systems and Organizations,* SP 800-53, Rev. 5 (Sept. 2020).

Table 4: Evaluation Criteria Associated with Key Cloud Security Practices

Key practice	Evaluation criteria
Continuous monitoring: Agency develops and implements a plan for continuously monitoring the security controls that are the agency's responsibility and performs regular reviews of continuous monitoring reports from the cloud service provider (provider), and monitors cloud infrastructure through vulnerability and audit log management.	Agency developed and implemented a plan for continuously monitoring the security controls that are the agency's responsibility.
	Agency regularly reviewed continuous monitoring deliverables from the provider.
	Agency used vulnerability management procedures and tools to monitor the agency's cloud infrastructure.
	Agency collected and reviewed audit logs
Incident response and recovery: Agency documents procedures for responding to and recovering from security and privacy incidents for the cloud system.	Agency had plans or procedures for identifying, containing, and mitigating cloud security incidents.
	Agency had plans or procedures for coordinating with providers and the Cybersecurity and Infrastructure Security Agency.
	Agency had plans or procedures for ensuring providers report security incidents promptly.
	Agency had plans or procedures for measuring and tracking incident response time.
	Agency had plans or procedures for testing of incident response and recovery procedures.
Service level agreements (SLA): Agency has an SLA with the provider that defines the level of service and performance expected from a provider, how that performance will be measured, and what enforcement mechanisms will be used to ensure the specified performance levels are achieved.	Agency's SLA with the provider defined performance metrics.
	Agency's SLA with the provider defined how the performance would be measured.
	Agency's SLA with the provider defined the enforcement mechanisms to ensure the specified performance levels are achieved.

Source: GAO analysis of federal law and guidance. | GAO-26-108443

We administered the standard set of questions to the four agencies on their implementation of key cloud-related security practices for selected systems. Each agency was asked to provide documentation related to the implementation of the cloud security practices for two of its cloud systems, one platform as a service system and one software as a service system.[7] We did not include infrastructure as a service systems in our review as it is the least common cloud model in the FedRAMP Marketplace. The documentation obtained included policies and cloud system artifacts such as continuous monitoring plans, incident response plans, reports from continuous monitoring tools, and service level agreements. We analyzed the documents to determine whether agencies addressed the evaluation criteria in each key practice area. We also

[7]Due to sensitivity concerns, we are not disclosing system names in this report and identify systems only by their cloud service model.

interviewed cognizant agency officials to obtain their views and verify the information provided.

For each system, we assessed each agency's implementation of our evaluation criteria within each key practice area as follows:

- **Fully implemented**: the agency provided evidence which showed that it fully 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, or provided evidence insufficient to demonstrate implementation of any criteria.

To determine an overall rating for each system within each of the three key practice areas, we 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 all criteria.
- **Not implemented**: the agency did not provide evidence that it had implemented any part of the evaluation criteria.

We conducted this performance audit from April 2025 to June 2026 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Appendix II: Comments from the U.S. Department of State

United States Department of Sta

Washington, D.C. 20520

JUN 04 2026

Kimberly Gianopoulos
Managing Director
International Affairs and Trade
Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548-0001

Dear Ms. Gianopoulos:

We appreciate the opportunity to review your draft report, "CYBERSECURITY: Selected Agencies Need to Better Protect Cloud Data." GAO Job Code 108443.

The enclosed Department of State comments are provided for incorporation with this letter as an appendix to the final report.

Sincerely,

Robert Collins
Deputy Executive Director, Executive,
Office of the Under Secretary for Management

Enclosure:
As stated

cc: GAO – David B. Hinchman
OIG - Norman Brown

Department of State Comments on GAO Draft Report

CYBERSECURITY: Selected Agencies Need to Better Protect Cloud
(GAO-26-108443, GAO Code 108443)

The Department of State appreciates the opportunity to comment on GAO's draft report *"Cybersecurity: Selected Agencies Need to Better Protect Cloud Data."*

The Secretary of State should ensure that the agency fully implements continuous monitoring for its selected PaaS system, to include reviewing continuous monitoring deliverables from the cloud service provider. (Recommendation 1)

Department Response (May 2026): The Department has developed formal procedures to fully implement continuous monitoring for the ABR PaaS system, as documented in the Department of State FedRAMP Continuous Monitoring (ConMon) Process. This procedure describes how the Department retrieves Microsoft's FedRAMP continuous monitoring deliverables through the Service Trust Portal, the Azure Federal Documentation (AzFedDoc) process, and the FedRAMP Marketplace. It also establishes a recurring review cadence for POA&Ms, scan results, deviation requests, and annual assessments. In addition, the procedure provides instructions for documenting reviews through checklists, meeting minutes, logs, and formal decisions, demonstrating the Department oversight of cloud service provider security artifacts. The Department will assess and implement any necessary changes identified through these reviews based on system scope, the criticality of findings, and assigned responsibilities.

The Secretary of State should ensure that the agency fully implements incident response and recovery for its selected PaaS system, to include documenting plans or procedures for coordinating incidents response and recovery with providers. (Recommendation 2)

Department Response (May 2026): The Department has established formal procedures for incident response and recovery for the ABR PaaS system, as documented in the *Department of State Incident Response Procedure (Draft)*. The procedure defines the coordination framework between the Department and Microsoft as the cloud service provider (CSP), including incident detection and classification, notification timeframes, required recipients, and the information Microsoft must provide in initial, follow-up, and final incident reports. It also

outlines FedRAMP obligations, assigns Department responsibilities for receiving notifications and initiating internal incident response processes, and specifies how these procedures are incorporated into the ABR System Security Plan (SSP). Together, these elements document how the Department and its PaaS provider coordinate incident reporting, escalation, response, and post-incident remediation.

Appendix III: Comments from the U.S. Department of Transportation

U.S. Department of Transportation
Office of the Secretary of Transportation

Assistant Secretary for Administration

1200 New Jersey Avenue, SE
Washington, D.C. 20590

May 26, 2026

David Hinchman
Director, Information Technology & Cybersecurity Team
U.S. Government Accountability Office
441 G Street NW
Washington, D.C. 20548

Dear Mr. Hinchman:

Improving the cybersecurity posture and capabilities of the U.S. Department of Transportation (DOT or Department) is an ongoing priority for the DOT Office of the Chief Digital and Information Officer (OCDIO). Over the last year, there have been significant improvements in the planning, execution, and delivery of enhancements, such as the establishment of a dedicated program and funding in the agency budget for the DOT Cybersecurity Initiative. For cloud services, the Department has effectively implemented key cloud security practices—continuous monitoring, incident response and recovery, and service level agreements. OCDIO is committed to working with cloud service providers to implement information security controls effectively to reduce risks to agency systems.

Upon review of the draft, the Department non-concurs with GAO's recommendation to ensure that DOT fully implements continuous monitoring for its selected SaaS system, including documenting the use of vulnerability management tools. Under the shared responsibility model established for the selected FedRAMP authorized cloud system, DOT does not maintain operational responsibility for performing vulnerability scans, using scanning tools, or remediating technical findings within the Software-as-a-Service (SaaS) environment. According to the Customer Responsibility Matrix provided by the FedRAMP authorized Cloud Service Provider (CSP), FedConnect, these specific technical controls—including executing authenticated scans, using scanning tools, and patching the underlying infrastructure—reside strictly within the purview of the CSP. DOT's role is governed by a governance and oversight framework rather than hands-on technical execution. Specifically, DOT fulfills its continuous monitoring (ConMon) obligations by participating in the FedRAMP authorized CSP's monthly ConMon meetings to review and assess the provider's security posture. Furthermore, DOT manages residual risk by documenting relevant ConMon weaknesses within the system's Plan of Action and Milestones and consistently updating the cloud system risk table. This ensures that while FedConnect manages cloud security, DOT remains responsible for security in the cloud through diligent risk management and administrative oversight. On May 5, 2026, the Department provided GAO with additional evidence and requested the finding and recommendation be omitted or closed upon issuance of the final report.

DOT appreciates the opportunity to respond to the GAO draft report. Please contact Gary Middleton, Director of Audit Relations and Program Improvement, at gary.middleton@dot.gov with any questions or if GAO would like to obtain additional information.

Sincerely,

Dr. Anne Byrd
Assistant Secretary for Administration

Appendix IV: Comments from the Department of Veteran Affairs

DEPARTMENT OF VETERANS AFFAIRS
WASHINGTON

June 4, 2026

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

Dear Mr. Hinchman:

The Department of Veterans Affairs (VA) reviewed the Government Accountability Office (GAO) draft report, ***Cybersecurity: Selected Agencies Need to Better Protect Cloud Data*** (GAO-26-108443).

The enclosure contains the action plan to address the draft report recommendations. VA appreciates the opportunity to comment on your draft report.

Sincerely,

Curt Cashour
Chief of Staff

Enclosure

Enclosure

Department of Veterans Affairs (VA) Comments to the
Government Accountability Office (GAO) Draft Report
Cybersecurity: Selected Agencies Need to Better Protect Cloud Data
(GAO-26-108443)

Recommendation 4: The Secretary of Veterans Affairs should ensure that the agency fully implements continuous monitoring for its selected PaaS system, to include collecting and reviewing audit logs.

VA Response: Concur. The Department of Veterans Affairs (VA) is committed to ensuring the security of VA's cloud systems. VA's Office of Information and Technology (OIT) implemented continuous monitoring for the selected Platform as a Service (PaaS) system through monthly reviews which follow Federal Risk and Authorization Management Program (FedRAMP) guidelines and contract requirements.

To further strengthen continuous monitoring for external VA cloud applications, including VA's PaaS system, OIT is deploying a new monitoring system – the Secure Access Service Edge (SASE) solution – which will provide continuous session verification, real-time threat protection, data protection, and user and entity behavior analytics.

To address the requirement for visibility into the internal environment of external solutions, OIT is also pursuing a solution to monitor and log internal third-party breaches. The SASE solution and the solution for monitoring and logging internal third-party breaches will enhance VA's ability to continuously monitor the selected PaaS system, to include collecting and reviewing audit logs. OIT anticipates implementing this solution for all external cloud applications by November 2026.

Target completion date: November 30, 2026.

Recommendation 5: The Secretary of Veterans Affairs should ensure that the agency fully implements continuous monitoring for its selected SaaS system, to include collecting and reviewing audit logs.

VA Response: Concur. VA OIT has implemented continuous monitoring for the selected Software as a Service (SaaS) system through monthly reviews which follow FedRAMP guidelines and contract requirements.

To further strengthen continuous monitoring for external VA cloud applications, including VA's SaaS system, OIT is deploying a new monitoring system – the SASE solution – which will provide continuous session verification, real-time threat protection, data protection, and user and entity behavior analytics.

To address the requirement for visibility into the internal environment of external solutions, OIT is also pursuing a solution to monitor and log internal third-party breaches. The SASE solution and the solution for monitoring and logging internal third-party breaches will enhance VA's ability to collect and review audit logs for the selected

Enclosure

Department of Veterans Affairs (VA) Comments to the
Government Accountability Office (GAO) Draft Report
Cybersecurity: Selected Agencies Need to Better Protect Cloud Data
(GAO-26-108443)

SaaS system. OIT anticipates implementing this solution for all external cloud applications by November 2026.

Target completion date: November 30, 2026.

Recommendation 6: The Secretary of Veterans Affairs should ensure that the agency fully implements incident response and recovery for its selected PaaS system, to include documenting plans or procedures for measuring and tracking incident response time.

VA Response: Concur. VA OIT has established incident response logging through enterprise security information and event management. The selected PaaS system provides an annual incident response plan and an information system contingency plan which are both updated annually as required by FedRAMP and the VA contract requirements.

To further strengthen incident response and recovery for the selected PaaS system, OIT will continue the process of onboarding applications to the SASE solution and enabling the System for Cross-Domain Identity Management (SCIM) connection. Full implementation of the SASE solution will enhance VA's capability to document plans and procedures for measuring and tracking incident response time.

Target completion date: November 30, 2026.

Recommendation 7: The Secretary of Veterans Affairs should ensure that the agency fully implements incident response and recovery for its selected SaaS system, to include documenting plans or procedures for testing incident response and recovery procedures.

VA Response: Concur. VA OIT has already established incident response logging through enterprise security information and event management. The selected SaaS system provides an annual incident response plan and an information system contingency plan which are both updated annually as required by FedRAMP and the VA contract.

To further strengthen incident response and recovery for the selected SaaS system, OIT will continue the process of onboarding applications to the SASE solution and enabling the SCIM connection. Full implementation of the SASE solution will enhance VA's capability to document plans and procedures for measuring and tracking incident response time.

Target completion date: November 30, 2026.

Enclosure

Department of Veterans Affairs (VA) Comments to the
Government Accountability Office (GAO) Draft Report
Cybersecurity: Selected Agencies Need to Better Protect Cloud Data
(GAO-26-108443)

Recommendation 8: The Secretary of Veterans Affairs should ensure that the agency's service level agreements with providers define performance metrics, including how they are measured and the enforcement mechanisms.

VA Response: Concur. VA's contracts with providers for SaaS and PaaS systems include defined performance metrics. In the 180-day update to the final report, VA will provide details on actions to address how VA measures service level agreement performance and utilizes enforcement mechanisms.

Appendix V: GAO Contact and Staff Acknowledgments

GAO Contact

David B. Hinchman, HinchmanD@gao.gov

Staff Acknowledgments

In addition to the individual named above, the following staff made key contributions to this report: Neelaxi Lakhmani (Assistant Director), Lee Hinga (Analyst in Charge), Chris Businsky, Kristi Dorsey, Jonnie Genova, and Philip Menchaca.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on X, LinkedIn, Instagram, and YouTube.
Subscribe to our Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454

Media Relations

Sarah Kaczmarek, Managing Director, Media@gao.gov

Congressional Relations

David A. Powner, Acting Managing Director, CongRel@gao.gov

General Inquiries

https://www.gao.gov/about/contact-us