United States Government Accountability Office

Report to the Committee on Oversight and Government Reform
House of Representatives

June 2026

CLOUD COMPUTING

Federal Government Needs to Address Procurement Challenges

GAO-26-107530

GAO Highlights

CLOUD COMPUTING

Federal Government Needs to Address Procurement Challenges

GAO-26-107530 June 2026

A report to the Committee on Oversight and Government Reform, House of Representatives

For more information, contact: Carol C. Harris at HarrisCC@gao.gov

What GAO Found

Senior agency officials from 22 of 24 selected agencies reported primarily relying on historical procurement data to help make cloud decisions. Timely implementation of the many recommendations GAO has made to federal agencies to improve these data could result in high-quality information.

Senior officials in the 24 agencies most frequently reported the following cloud procurement challenges.

Challenges Reported by 24 Selected Federal Agencies on Cloud Procurement

Challenge identified	Number of agencies reporting challenge
Control of cloud costs required changes in IT management approaches.	17
Conflicting Office of Management and Budget and National Institute of Standards and Technology-issued software guidance caused confusion.	17
Outdated Federal Acquisition Regulations impeded cloud procurements.	15
Agencies encountered difficulties in obtaining authorized cloud solutions.	15
Multi-vendor cloud adoption faced new technical considerations such as interoperability.	11
Resource constraints hindered cloud workforce acquisition.	10

Source: GAO analysis of agency interviews and federal guidance documentation. | GAO-26-107530

Agencies are addressing challenges in controlling cloud costs, obtaining authorized cloud solutions, and issuing guidance and responding to cloud staffing limitations. Agencies' ongoing and planned actions, if implemented effectively, demonstrate promise for tackling these challenges and could lead to substantial savings.

In contrast, the challenges of conflicting software guidance, outdated Federal Acquisition Regulations (FAR), and multi-vendor cloud solutions remain.

- The Office of Management and Budget (OMB) and National Institute of Standards and Technology issued conflicting guidance to agencies that created unnecessary burdens for collecting and storing key software components. The Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency is well positioned to address this conflict by providing additional guidance on implementation to agencies.
- The FAR remains out of date in areas impacting cloud procurement. Although significant changes were made to the FAR between April 2025 and October 2025, the FAR still does not have a definition of cloud computing, the definition of IT is 20 years old, and the definition of a commercial product or service does not align with cloud computing. Updating the FAR to reflect present day computing is essential to effectively contracting for cloud services.
- Several larger agencies are using multiple cloud vendors to achieve efficiencies but are also experiencing new challenges such as interoperability. Sharing multi-cloud leading practices would enable other agencies to learn from each other and improve implementation efforts.

Why GAO Did This Study

Federal IT acquisitions of cloud services have the potential to reduce costs and improve operational efficiencies. Cloud computing enables on-demand access to shared computing resources. Cloud services use a consumption-based model, and providers generally bill customers based on actual usage of resources (i.e., data storage, computing power, backup, development tools, applications).

GAO was asked to review agencies' efforts to address cloud procurement. This report assesses, among other things, (1) the cloud procurement data agencies and OMB use and collect to inform acquisition decision making, and (2) agency challenges procuring cloud services and efforts to address the challenges. For each of the 24 Chief Financial Officers Act agencies, GAO analyzed relevant cloud procurement data, policies, and guidance. Further, GAO interviewed senior officials in the 24 agencies' Offices of the Chief Information Officer (CIO) and Senior Procurement Executive. GAO also interviewed staff in OMB's Office of the Federal CIO and Office of Federal Procurement Policy and staff in the General Services Administration's (GSA) Office of Government-wide Policy and Federal Acquisition Service.

What GAO Recommends

Congress should consider requiring changes to the FAR to update cloud-related definitions. GAO is also making three recommendations to GSA, DHS, and the Federal CIO Council to address cloud cost management practices, conflicting cloud guidance, and multi-vendor cloud solutions. DHS concurred with our recommendation, GSA disagreed with our recommendation, and the CIO Council did not provide comments. GAO maintains that its recommendations are warranted.

Contents

Figures

Abbreviations

CIO	chief information officer
CISA	Cybersecurity and Infrastructure Security Agency
CSP	cloud service provider
DHS	Department of Homeland Security
DHS PIL	Department of Homeland Security Procurement Innovation Laboratory
DOD	Department of Defense
EPA	Environmental Protection Agency
FAR	Federal Acquisition Regulation
FAR Council	Federal Acquisition Regulatory Council
FAS	Federal Acquisition Service
FedRAMP	Federal Risk and Authorization Management Program
FinOps	Financial Operations
FITARA	Federal Information Technology Acquisition Reform Act
FPDS	Federal Procurement Data System
GSA	General Services Administration
GWAC	government-wide acquisition contract
HHS	Department of Health and Human Services
HUD	Department of Housing and Urban Development
IaaS	infrastructure as a service
IT	information technology
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
NSF	National Science Foundation
OFPP	Office of Federal Procurement Policy
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PaaS	platform as a service
PIL	procurement innovation laboratory
PSC	product and service code

SaaS	software as a service
SAM	System for Award Management
SBA	Small Business Administration
SBOM	software bill of materials
SSA	Social Security Administration
USAID	U.S. Agency for International Development
VA	Department of Veterans Affairs

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

June 23, 2026

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

Federal agency IT provides essential services affecting the health, economy, and defense of the nation, serving as a foundation for the federal government's ability to deliver on its mission. Accordingly, agencies need to maximize the impact of taxpayer dollars and make procurement decisions that deliver on their missions securely and reliably. These investments also have the potential to make agencies more efficient in fulfilling their missions by reducing costs and improving operational efficiencies. In fiscal year 2025, the President's proposed federal budget described plans to spend about $140 billion on IT investments.[1]

For several decades, we have reported that federal IT investments too frequently fail or incur cost overruns and schedule delays while contributing little to mission-related outcomes.[2] Because of these longstanding challenges, we added the federal government's management of IT acquisitions and operations to our high-risk list as a government-wide challenge in February 2015.[3] Underscoring the significance of the issues agencies face in effectively acquiring and managing IT, we have continued to designate the management of IT acquisitions and operations as a high-risk area in each of our high-risk

[1]Office of Management and Budget, *Analytical Perspectives, Budget of the U.S. Government, Fiscal Year 2025* (Washington, D.C.: Mar. 11, 2024); Department of Defense, *Department of Defense Information Technology and Cyberspace Activities Budget Overview: President's Budget 2025 Budget Request* (March 2024).

[2]GAO, *Information Technology: OMB and Agencies Need to More Effectively Implement Major Initiatives to Save Billions of Dollars*, GAO-13-796T (Washington, D.C.: July 25, 2013); U.S. General Accounting Office, *Government Reform: Legislation Would Strengthen Federal Management of Information and Technology*, GAO/T-AIMD-95-205 (Washington, D.C.: July 25, 1995); *Information Technology Utilization by the Federal Government*, GAO/T-IMTEC-89-9 (Washington, D.C.: June 12, 1989); and *Effective Management of Computer Leasing Needed to Reduce Government Costs*, GAO/IMTEC-85-3 (Washington, D.C.: Mar. 21, 1985).

[3]GAO, *High-Risk Series: An Update*, GAO-15-290 (Washington, D.C.: Feb. 11, 2015).

series updates since then.[4] Our February 2025 report highlighted IT challenges in workforce, portfolio oversight and management, and acquisition practices that continue to persist.[5]

Recognizing the need 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 service (cloud services) option when feasible.[6] 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 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.

In June 2019, OMB published its updated *Federal Cloud Computing Strategy*, called Cloud Smart, to accelerate agency adoption of cloud services.[7] The strategy focused on equipping agencies with the tools needed to make informed IT decisions according to their mission needs. It identified procurement as one of the three key pillars for successful cloud adoption needed to deliver high quality services and improve the return on agencies' cloud investments.[8]

You asked us to review agencies' efforts to procure cloud computing solutions. Our objectives were to (1) assess the cloud procurement data

[4]GAO, *High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas*, GAO-23-106203 (Washington, D.C.: Apr. 20, 2023); *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas*, GAO-21-119SP (Washington, D.C.: Mar. 2, 2021); *High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas*, GAO-19-157SP (Washington, D.C.: Mar. 6, 2019); and *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*, GAO-17-317 (Washington, D.C.: Feb.15, 2017).

[5]GAO, *High-Risk Series: Heightened Attention Could Save Billions More and Improve Government Efficiency and Effectiveness*, GAO-25-107743 (Washington, D.C.: Feb. 25, 2025).

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

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

[8]OMB's *Federal Cloud Computing Strategy* identified security and workforce as the other two key pillars for successful cloud adoption.

that agencies and OMB collect and use to inform decision-making on cloud acquisitions, (2) identify agency leading practices for procuring cloud services and any government-wide efforts to adopt the practices, and (3) assess agency cloud procurement challenges and government-wide efforts to address the challenges.

To address these objectives, we selected the 24 covered agencies for this review because these agencies were all required to implement Cloud Smart.[9] These agencies were the Department of Agriculture, Department of Commerce, Department of Defense (DOD), Department of Education, Department of Energy, Department of Health and Human Services (HHS), Department of Homeland Security (DHS), Department of Housing and Urban Development (HUD), Department of the Interior, Department of Justice, Department of Labor, Department of State, Department of Transportation, Department of the Treasury, Department of Veterans Affairs (VA), Environmental Protection Agency (EPA), General Services Administration (GSA),[10] National Aeronautics and Space Administration (NASA), National Science Foundation (NSF), Nuclear Regulatory Commission (NRC), Office of Personnel Management (OPM), Small Business Administration (SBA), Social Security Administration (SSA), and the U.S. Agency for International Development (USAID).

For the first objective, we analyzed agencies' documentation describing the use of cloud procurement data and descriptions of key cloud procurement data practices. We also assessed the reliability of the 24

[9]The term covered agency refers to the 24 major agencies listed in the Chief Financial Officers Act of 1990. 31 U.S.C. § 901(b).

[10]As part of our review, we interviewed officials from GSA's Office of the Chief Information Officer (CIO) regarding the agency's cloud procurement efforts, data, practices and challenges. We also interviewed officials from GSA's Office of Government-wide Policy, the Federal Acquisition Service (FAS), and the Project Management Office for the Federal Risk and Authorization Management Program (FedRAMP) regarding federal cloud procurement strategy and federal cloud contracting. We interviewed them regarding any planned or ongoing government-wide efforts to promote the agency-reported best practices or address the agency-reported challenges. For reporting purposes, we refer to GSA officials when discussing the agency's procurement efforts and identify the specific GSA office when referring to GSA officials that were speaking about government-wide activities.

agencies' Federal Procurement Data System (FPDS) cloud service data[11] because OMB stated that OMB used these data to make decisions regarding cloud procurements.[12] Based on our assessment of the data and the measures that we took to assess the reliability of the data reported in FPDS, we determined that FPDS cloud data were not sufficiently precise for determining aggregated cloud spending. We therefore did not include the amounts obligated on cloud contracts in our report.

On February 24, 2026, GSA retired the FPDS.gov website and its ezSearch tool, migrating federal procurement data into the System for Award Management (SAM). SAM.gov is an integrated award environment hosted by GSA. Our analysis of FPDS data was conducted prior to the migration of the system into SAM.gov in February 2026. For the purpose of this report, we discuss the FPDS policies that were current as of February 2026 because these were in place when we conducted our audit work with the 24 agencies in our review.

We also interviewed senior officials from each of the 24 agencies from the offices of the Chief Information Officer (CIO), the Senior Procurement Executive, the Chief Acquisition Officer, the Chief Financial Officer, and other components in charge of cloud services. We sought information regarding the agency's use of cloud procurement data and the decisions made using these data. Further, we interviewed staff from OMB's Office of the Federal CIO and Office of Federal Procurement Policy (OFPP).

To address the second objective, we reviewed prior GAO cloud and procurement reports; federal and agency procurement guidance; laws

[11]To assess FPDS reliability, we: (1) assessed FPDS data to determine whether it was complete and accurate, and (2) reviewed prior GAO reports that identified challenges with the reliability of the data. We synthesized the information from these reports to identify common themes affecting the reliability of the data. We also reviewed supporting FPDS documentation and interviewed staff within GSA responsible for the management of the system. See appendix I for more details.

[12]Prior to February 24, 2026, FPDS was a key source for U.S. government-wide procurement data and provided a comprehensive web-based tool for agencies to report contract actions. It also provided a public website and ezSearch tool that allowed the public and other users to look up contract awards and agency procurement activity. Through the *Office of Federal Procurement Policy Act of 1974*, Congress mandated that contract actions using appropriated funds must be reported to FPDS, the central repository of information on federal contracting. The Office of Federal Procurement Policy (OFPP), under OMB, has been responsible for issuing guidance and policy related to FPDS, including how data is collected and used. GSA has administered FPDS on behalf of OFPP.

and regulations; and procurement processes and contracts for cloud service acquisition, workforce, and cloud services. We synthesized the information to develop a list of 16 topic areas that aligned with the key activities in a federal competitive acquisition process. We interviewed senior officials from each of the 24 agencies from the offices of the CIO, the Senior Procurement Executive, the Chief Acquisition Officer, the Chief Financial Officer, and other components in charge of cloud services regarding the agency's procurement practices. We discussed with senior officials whether the agency had identified leading practices in the 16 topic areas or had other leading practices in additional areas related to cloud procurement. To develop the list of practices, we reviewed the interview responses, agency-provided documentation, federal leading practice guidance, and prior related reports since 2010. We chose 2010 because that was the first year that agencies were required to begin using cloud services. We distilled the information into a list of three practices and totaled the number of agencies that had reported them. We presented our analysis to the agencies for confirmation and incorporated their feedback.

To address the third objective, we reviewed prior GAO cloud computing and procurement reports; federal or agency procurement guidance; laws and regulations; and procurement processes for cloud services. Using the same list of 16 topic areas discussed in our second objective, we interviewed senior officials from each of the 24 agencies from the offices of the CIO, the Senior Procurement Executive, the Chief Acquisition Officer, the Chief Financial Officer, and other components in charge of cloud services regarding the agency's procurement challenges. We discussed with senior officials if the agency had identified challenges in the 16 areas or had other procurement challenges.

To develop the list of challenges, we reviewed interview responses, agency-provided guidance and lessons learned documentation, and prior related reports since 2010. We distilled the information into a list of six challenges and totaled the number of agencies that had reported them. We confirmed the information with agencies and incorporated their feedback as appropriate.

We also interviewed OMB staff from the Office of the Federal CIO and OFPP and GSA staff from the Office of Government-wide Policy, Federal Acquisition Service (FAS), and the Project Management Office for the Federal Risk and Authorization Management Program (FedRAMP). We sought information regarding federal cloud procurement strategy and any

planned or ongoing government-wide efforts to promote the key practices or address the challenges as of March 2025.

Beginning in March 2025, the President issued three executive orders that impacted federal agency cloud procurement efforts.[13] Specifically:

- Executive Order 14240, *Eliminating Waste and Saving Taxpayer Dollars by Consolidating Procurement,* was issued on March 20, 2025.[14] The order directed that the acquisition of federal goods and services be centralized under GSA. The executive order further directed that GSA take over government-wide acquisition contracts (GWAC) for information technology.
- Executive Order 14275, *Restoring Common Sense to Federal Procurement*, was issued on April 15, 2025.[15] The executive order directed OFPP, in coordination with the Federal Acquisition Regulatory Council (FAR Council) and others, to reduce the Federal Acquisition Regulation (FAR) to only what was required by statute and was necessary for streamlined and efficient federal procurement. The FAR is currently undergoing a complete overhaul called the Revolutionary FAR Overhaul.
- Executive Order 14271, *Ensuring Commercial, Cost-Effective Solutions in Federal Contracts*, was also issued on April 15, 2025.[16] The order directed agencies to procure commercially available products and services to the maximum extent practicable.

Much of our analysis was conducted prior to the Revolutionary FAR Overhaul and GSA's consolidation efforts. For the purposes of this report,

[13]In April 2026, the President issued Executive Order 14402, *Promoting Efficiency, Accountability, and Performance in Federal Contracting.* The order stated that it was the policy of the administration that fixed-price contracts with performance-based considerations should serve as the default and preferred method of procurement for the federal government. In addition, the order noted that using fixed-price contracts would ensure that advanced cost predictability, budget discipline, appropriate contractor incentives and accountability, and streamlined procurement and contract administration would incentivize performance rather than cost inflation. See Exec. Order No. 14402, *Promoting Efficiency, Accountability, and Performance in Federal Contracting* (91 Fed. Reg. 24325 (May 5, 2026).

[14]Exec. Order No. 14240, *Eliminating Waste and Saving Taxpayer Dollars by Consolidating Procurement*, 90 Fed. Reg. 13671 (Mar. 20, 2025).

[15]Exec. Order No. 14275, *Restoring Common Sense to Federal Procurement*, 90 Fed. Reg. 16447 (Apr. 15, 2025).

[16]Exec. Order No. 14271, *Ensuring Commercial, Cost-Effective Solutions in Federal Contracts*, 90 Fed. Reg. 16433 (Apr. 15, 2025).

we discuss the FAR policies and procedures that were current as of March 2025 in our analysis of the agency procurement practices and challenges.[17] We chose March 2025 because these regulations were in place when we conducted our audit work with the 24 agencies in our review. Significant changes to the FAR were made between April 2025 and October 2025.[18] We also discuss these changes to the FAR as of October 2025 in the report. Further details on our objectives, scope, and methodology are included in appendix I.

We conducted this performance audit from April 2024 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

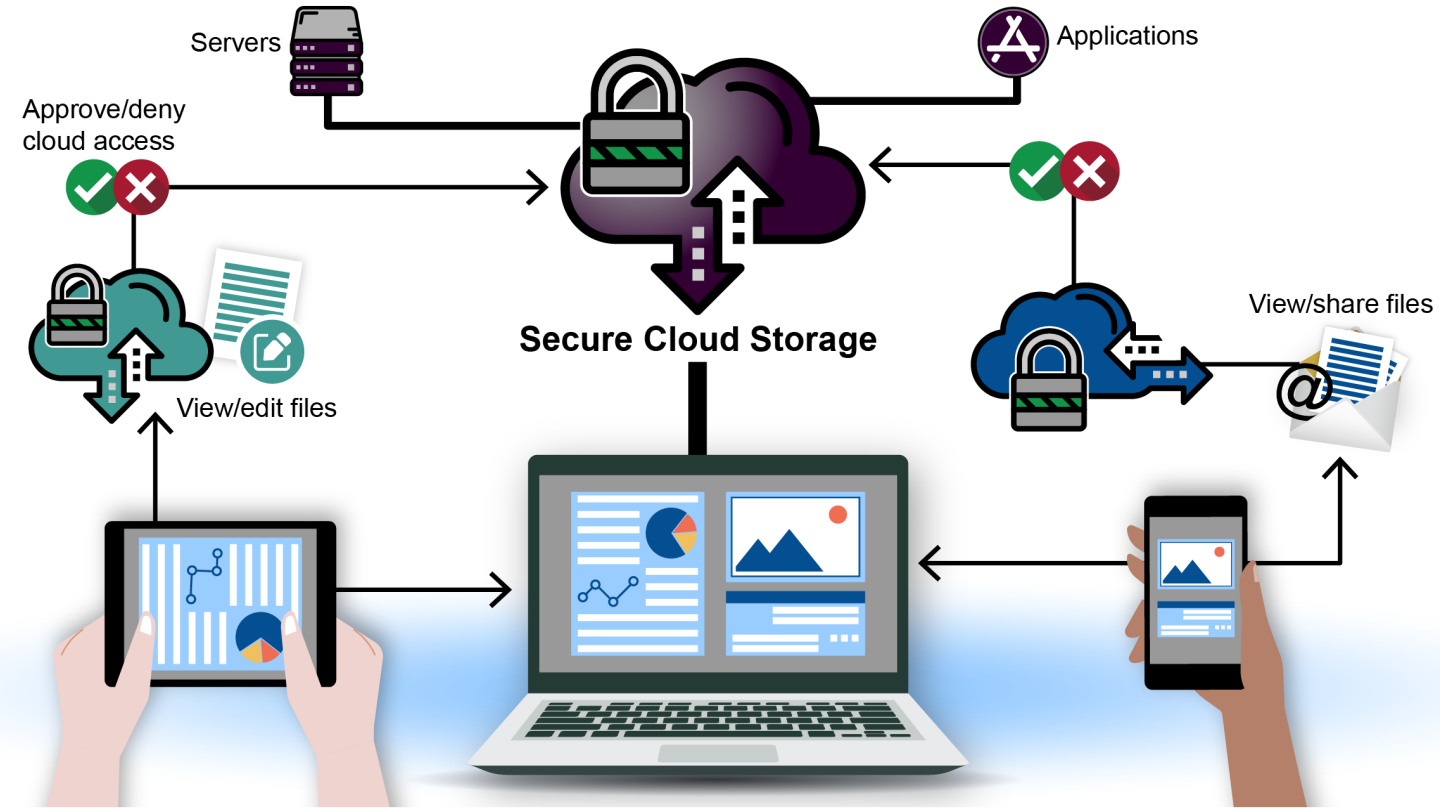
Background

According to 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. More specifically, purchasing IT services through a cloud service provider (CSP) enables agencies to avoid paying for all the computing resources that would typically be needed to provide such services. This approach 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. Figure 1 provides an illustration of a cloud computing environment.

[17]For the purposes of this report, we refer to the March 2025 version as the FAR (legacy), and the Revolutionary FAR Overhaul version as the FAR (deviation).

[18]Phase One of the Revolutionary FAR Overhaul was completed in October 2025.

Figure 1: Illustration of a Cloud Computing Environment



Sources: GAO analysis of data from the Cybersecurity and Infrastructure Security Agency, General Services Administration, and National Institute of Standards and Technology; GAO (other icons/illustrations); 32 pixels/stock.adobe.com (cloud and lock illustrations); ST.art/stock.adobe.com (computer, phone and hands illustration). | GAO-26-107530

According to NIST, cloud computing offers federal agencies a number of benefits:[19]

- **On-demand self-service.** Agencies can, as needed, provision computing capabilities, such as server time and network storage, from the service provider automatically and without human interaction.
- **Broad network access.** Agencies can access needed capabilities over the network through workstations, laptops, or other mobile devices.
- **Resource pooling.** Agencies can use pooled resources from the cloud provider, including storage, processing, memory, and network bandwidth.

[19]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 (Sept. 2011).

- **Rapid elasticity.** Agencies can provision the resources that are allocated to match what actual resources are needed according to demand. This is done by scaling resources up or down by adding or removing processing or memory capacity, or both, according to demand.
- **Measured service.** Agencies can pay for services based on usage. This allows agencies to monitor, control, and generate reports, providing greater transparency into the agency's use of cloud services.

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. NIST has identified three primary cloud service models, each of which has unique features and security implications.[20]

- **Infrastructure as a Service (IaaS)** includes infrastructure for functions such as data storage, computing power, and backup and recovery services. The service provider delivers and manages the basic computing infrastructure of servers, software, storage, and network equipment. The organization manages the operating system, programming tools and services, and applications. An organization and its IaaS provider generally share security responsibilities for data, identity and access management, and networking.
- **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 and operating system while providing software development kits or other PaaS tools the organization can use to develop applications. An organization and its PaaS provider generally share security responsibilities for data, identity and access management, networking, and 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 organization can use on demand. An organization and its SaaS provider generally share security responsibilities for data and identity and access management.

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

NIST has also defined four types of cloud deployment models:

- **Private cloud.** 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 customer's premises.
- **Community cloud.** 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 organization's premises.
- **Public cloud.** Service is available to the general public and is owned and operated by the service provider.
- **Hybrid cloud.** 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.

Multi-Cloud Environments Have a Variety of Attributes

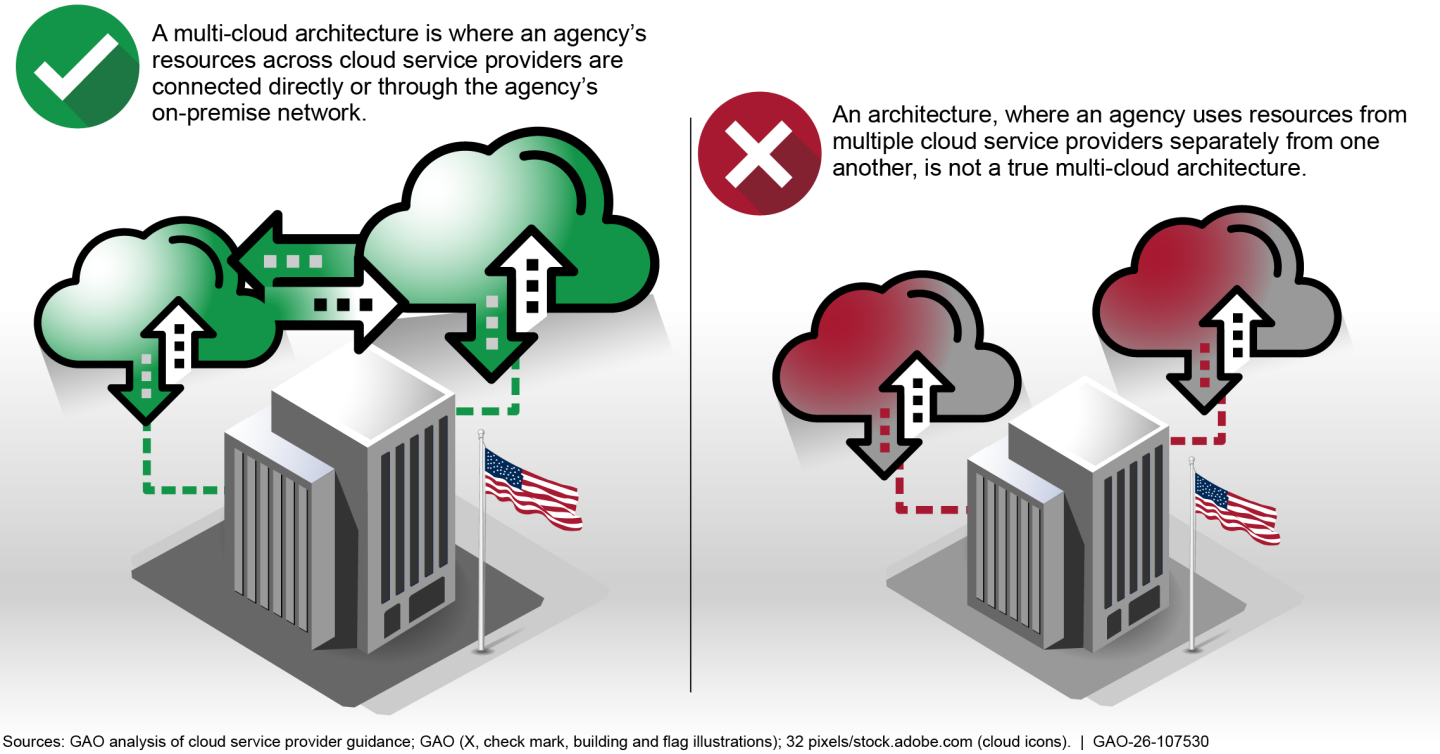
Agencies can also choose to use a multi-cloud strategy. A multi-cloud architecture refers to the use and integration of cloud services from multiple CSPs. While SaaS and PaaS can be part of a multi-cloud architecture, the term generally refers to IaaS offerings, where the customer is responsible for configuring the underlying compute, storage, network, and other foundational resources.

Importantly, a multi-cloud architecture involves the intentional integration of the different CSP offerings. One CSP may be used as backup infrastructure for an application hosted by another provider, or a portfolio of applications may be distributed among multiple providers with interoperable communication among the CSPs. In contrast, an architecture that uses multiple providers but does so in a non-interoperable fashion, would not be considered a multi-cloud environment. For example, different components of an agency may purchase services from different CSPs without coordinating with one another, resulting in networks that are unable to communicate with one another.

GSA guidance states that an agency could have cloud services from multiple cloud providers that serve the agency's enterprise. However, if the cloud services were created on an ad-hoc or patchwork basis, it

should not be considered a true multi-cloud architecture (see figure 2 below).[21]

Figure 2: Depiction of Multi-Cloud Architecture and Multiple Cloud Architecture



Sources: GAO analysis of cloud service provider guidance; GAO (X, check mark, building and flag illustrations); 32 pixels/stock.adobe.com (cloud icons). | GAO-26-107530

A multi-cloud strategy includes a range of advantages and potential challenges for agencies. For example, diversifying across multiple cloud platforms can help avoid vendor lock-in and mitigate the effects of potential service outages.[22] However, supporting multiple cloud platforms also increases costs associated with maintaining a skilled workforce due to the need for specialized expertise to use each cloud environment effectively.

[21]General Services Administration Office of Government-wide Policy, *Multi-Cloud and Hybrid Cloud Guide* (Sept. 3, 2021).

[22]Vendor lock-in describes the practice of platforms or technologies that "lock" customers into a particular product, limiting their ability to change vendors in the future.

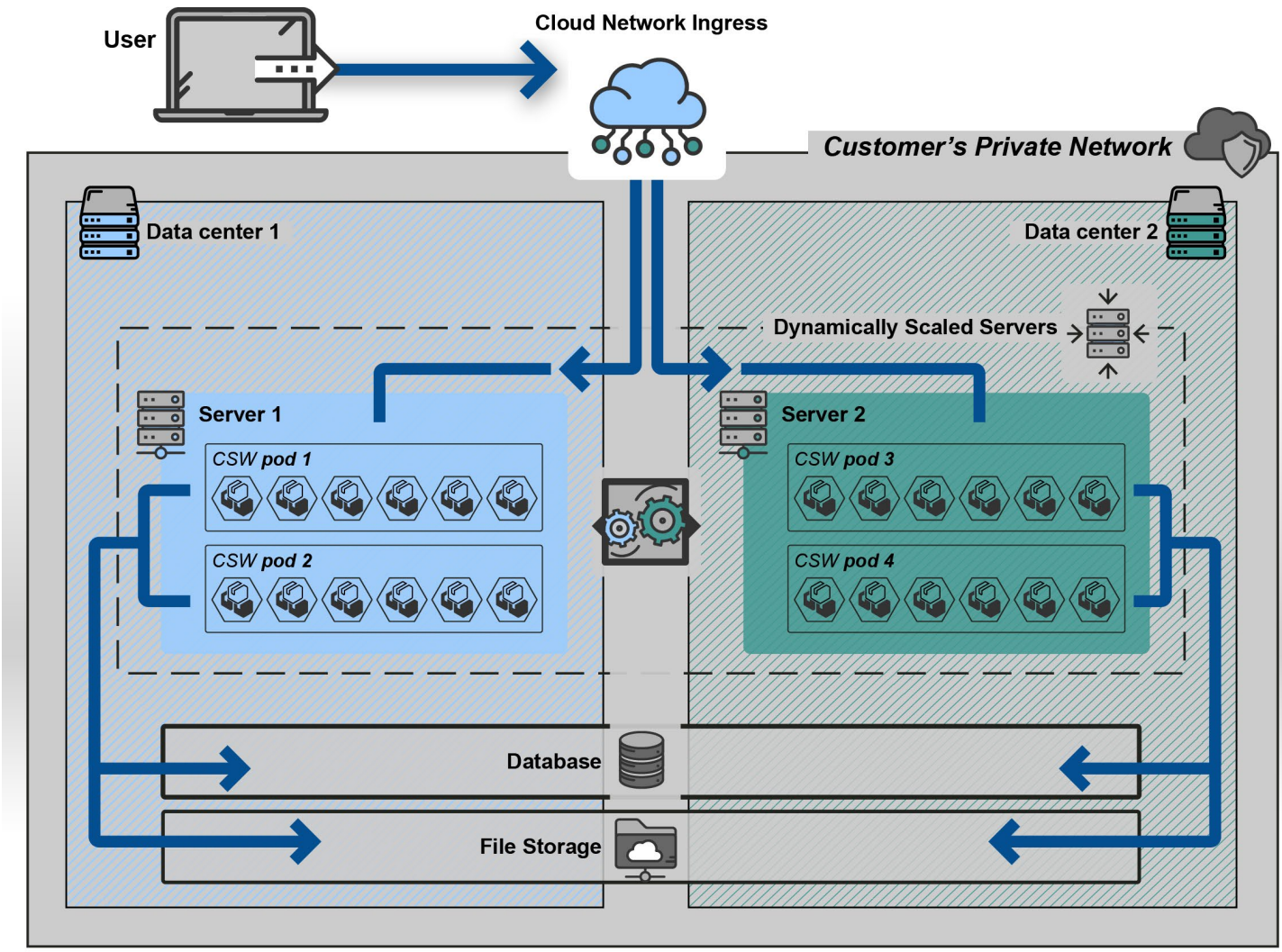
Containerization Helps Manage Complexity of Multi-Cloud Environments

Containerization allows software to be bundled together independently from the underlying hardware and operating system. Virtual machines share hardware resources with other virtual machines and replicate a full functioning operating system. Containers rely on the host's operating system to isolate and provide resources for the running software. This reliance on the host operating system enables container images to be much smaller and easier to run in different environments than a virtual machine.

This portability makes containerized software ideal for cloud environments. Many CSPs provide services that run containers between IaaS and PaaS environments. Providing these services allows the provider to take responsibility for the operation of the underlying server and operating system away from the customer. However, agencies must still address configuration issues. The underlying infrastructure of CSPs (networks, persistent storage, and identity and privilege management) and on-premise options can vary. Containers need to be configured to work with this infrastructure even if the container image running the software remains the same across all environments.

Container orchestration tools help address some of the challenges of managing containerized software at scale and enhance the benefits of containers. For example, container orchestration tools allow a developer to define how many instances of a particular containerized software they want running. If a server fails or a data center goes offline, the orchestration tool automatically creates a new version of the container on a different server or data center and redirects network traffic to the new container. These tools can help simplify some of the CSP-specific infrastructure that the containers rely on. These tools can also be run in a variety of cloud environments including on-premises or in a CSP, either as a managed service or through self-management, and in hybrid or multi-cloud strategies. In highly advanced use cases, an orchestration tool running on-premises or in a single provider can manage servers, containers, and infrastructure in multiple providers and data centers, assuming the agency has set up a proper multi-cloud architecture (see figure 3 below).

Figure 3: An Illustration of a Cloud Container Environment



Container Orchestrator moves pods among servers and causes (virtual) servers to be provisioned or destroyed as-needed.

CSW = containerized software

Sources: GAO analysis of GSA container orchestration guidance; 32 pixels/stock.adobe.com (all icons). | GAO-26-107530

However, these tools can be highly complex and difficult to manage. The interactions between the containers they orchestrate and the underlying infrastructure create novel cybersecurity risks. The tools require configurations and add-ons unique to each provider to provide the infrastructure to support the containers. In addition, while many CSPs

provide orchestration tools as a service, if the underlying orchestration tool is the same across providers, it will still need to be set up and managed specifically for the provider.

In addition to assessing technical considerations, agencies also need to consider the financial implications in determining how to implement cloud services. Cloud pricing models can be complex, with costs that vary based on size, expected consumption, and contractual negotiations, making it difficult to forecast spending in the long term. As a result, agencies must actively determine how to manage cloud spending (e.g., move to a consumption-based model or pay-as-you-go model).

Federal Oversight and Guidance for Cloud Services

OMB is tasked with overseeing federal agencies' management of information and IT, as well as procurement.[23] Within OMB, Congress has given primary responsibility for oversight of federal IT to the Administrator of the Office of Electronic Government and IT, who is also called the Federal CIO.[24] In addition, primary responsibility for oversight of federal procurement has been given to the Administrator of OFPP.[25] As a part of its oversight, OMB is responsible for developing and ensuring the implementation of policies and guidelines that drive enhanced technology performance, efficiency and effectiveness in government acquisitions, and budgeting for the federal government.

GSA has also been designated specific responsibility for technology and acquisition within the federal government.[26] Within GSA, the Office of Government-wide Policy is responsible for providing policy, guidance, best practices, and subject matter expertise related to technology to

[23]40 U.S.C. §§ 11302-03 (*Clinger-Cohen Act*); see also 44 U.S.C. § 3504 (*Paperwork Reduction Act*); 44 U.S.C. § 3602 (*E-Government Act*); 44 U.S.C. § 3553 (*Federal Information Security Modernization Act of 2014,* which largely superseded the *Federal Information Security Management Act of 2002*).

[24]OMB's Office of Electronic Government is to work with OMB's Office of Information and Regulatory Affairs in carrying out its IT management responsibilities. 44 U.S.C. § 3602.

[25]41 U.S.C. § 402 (*Office of Federal Procurement Policy Act Amendments of 1988*).

[26]40 U.S.C. § 101 et seq. Under Executive Order, *Eliminating Waste and Saving Taxpayer Dollars by Consolidating Procurement*, dated March 20, 2025, GSA is to oversee the procurement of common goods and services, including IT, with the GSA Administrator being designated as the executive agent for all government-wide acquisition contracts for information technology. Exec. Order No. 14240, *Eliminating Waste and Saving Taxpayer Dollars by Consolidating Procurement*, 90 Fed. Reg. 13671 (Mar. 20, 2025). GSA established the Office of Centralized Acquisition Services as the central hub for acquisition execution. The office is to support agencies as they transition authority for designated contracts to GSA, also known as GSA consolidation.

federal agencies. The FAS provides products, services, and solutions for the government, including technology and procurement and online acquisition tools.

The IT Vendor Management Office works to improve how the government buys common IT goods and services, including ensuring best pricing and eliminating duplicative contracts.[27] GSA also manages the Cloud and Infrastructure Community of Practice. The community of practice is designed for federal IT practitioners who want to network with other agencies to learn about common cloud, infrastructure, and IT challenges and best practices. GSA's IT Modernization Division supports this community of practice.[28]

Further, the Cybersecurity and Infrastructure Security Agency (CISA) within DHS is responsible for protecting federal civilian agencies' networks and systems from cyber threats and enhancing the security of the nation's critical infrastructure.[29] In carrying out its responsibilities, CISA has issued guidance in several areas, including cloud security and supply chain risk management. The agency is also responsible for maintaining a repository of software-related information and artifacts.[30]

Officials within each federal agency have also been given responsibility for technology and acquisition. Each of the 24 Chief Financial Officers Act agencies has a CIO that is responsible for IT management, governance, security, IT workforce, and systems acquisition, including cloud

[27]The IT Vendor Management Office also collaborated with the TBM Project Management Office to lead the Cloud Acquisitions Working Group, which collected best practices and use cases and prepared recommendations for enhancing public sector cloud acquisition efficiency in 2023.

[28]The IT Modernization division within GSA's Office of Government-wide Policy is to provide the 24 agencies with support and guidance for cloud strategy and datacenter optimization. GSA paused the Cloud and Infrastructure Community of Practice from February 2025 to April 2025.

[29]*Cybersecurity and Infrastructure Security Agency Act of 2018*, Pub. L. No. 115-278, § 2(a), 132 Stat. 4168, 4169-70, (Nov. 16, 2018) (adding section 2202 to the Homeland Security Act of 2002, Pub. L. No. 107-296 and codified in relevant part at 6 U.S.C. § 652(c)).

[30]CISA's Repository for Software Attestations and Artifacts was established in March 2024. Agencies submit information using a software attestation form created by CISA.

acquisition.[31] In addition, each of the 24 agencies is required to designate a Senior Procurement Executive who is responsible for the management direction of the agency's procurement system, including implementation of the agency's unique procurement policies, regulations, and standards.[32] Sixteen of the civilian agencies also have a Chief Acquisition Officer to advise and assist agency leadership to help ensure that the agency's mission is achieved through the management of its acquisition activities.[33]

In addition, the CIO Council is the principal interagency forum for improving agency practices connected to the acquisition, design, development, modernization, use, sharing, and performance of federal information resources. The Council is chaired by OMB's Deputy Director for Management and is comprised of federal agency CIOs. The Council manages the Federal Technology Investment Management Community of Practice. The community of practice comprises a group of cross-agency partners that mature the integration of Technology Business Management,[34] IT capital planning and IT investment control, and

[31]See 44 U.S.C. § 3506 (Federal agency responsibilities). Under the Executive Order, *Eliminating Waste and Saving Taxpayer Dollars by Consolidating Procurement*, dated March 20, 2025, the procurement of federal IT is to be consolidated within GSA. Exec. Order No. 14240, 90 Fed. Reg. 13671 (Mar. 20, 2025). However, under the Executive Order, OMB and the GSA Administrator can "defer or decline" being the executive agent of IT governmentwide contracts when necessary to ensure continuity of service or as otherwise appropriate.

[32]The Senior Procurement Executive position was established in 1983. 41 U.S.C. § 1702(c)(*Chief Acquisition Officers and senior procurement executives*).

[33]The position of the Chief Acquisition Officer was established under the *Services Acquisition Reform Act of 2003*. The position of the Chief Acquisition Officer was established under the *Services Acquisition Reform Act of 2003*. The law required executive agencies described in certain sections of the Chief Financial Officers Act of 1990, Pub. L. No. 101-576 (see, 31 U.S.C. §§ 901(b)(1) and 901(b)(2)(C) (CFO Act)), to appoint a Chief Acquisition Officer. In 2004, the *Department of Homeland Security Financial Accountability Act*, Pub. L. No. 108-330, § 3, amended the Chief Financial Officer Act to make a number of changes, including adding DHS to the list of agencies required to have a Chief Financial Officer. The *Services Acquisition Reform Act of 2003* exempts DOD from the Chief Acquisition Officer requirement. Legislation enacted prior to the *Services Acquisition Reform Act of 2003* required DOD to have an Under Secretary of Defense (now Under Secretary of Defense for Acquisition and Sustainment) who has responsibilities similar to those of a Chief Acquisition Officer.

[34]Technology Business Management is a framework that provides a common language for categorizing, comparing, and reporting IT spending. The taxonomy is organized into four layers that are intended to show an organization's total IT spending from different perspectives. OMB began requiring agencies to use the framework to report spending on agency investments, including cloud investments, starting in fiscal year 2019.

portfolio management practices in the federal government through the sharing of best practices and lessons learned.

In June 2019, OMB issued an update to its *Federal Cloud Computing Strategy*.[35] The strategy focused on equipping agencies with the tools needed to make informed IT decisions according to their mission needs. Regarding cloud procurement, the strategy noted that there remained a lack of consistency across agency implementations and information sharing on best practices. To address these challenges, the strategy said that agencies would need to use a variety of approaches that leveraged the strength of the federal government's bulk-purchasing power, and the shared knowledge of sound acquisition principles and relevant risk management practices. The strategy also noted that agencies needed to recruit and hire staff to address skill gaps in the cloud workforce. According to the strategy, agencies should continuously evaluate and update their recruitment and hiring strategies to include leveraging industry recruitment best practices, expanding the use of pay flexibilities, and removing bureaucratic barriers to hiring staff expeditiously.

OMB Guidance on FedRAMP

In December 2011, OMB launched FedRAMP to facilitate the adoption and use of cloud services. The program was intended to provide a standardized approach for selecting and authorizing the use of cloud services that met federal security requirements.[36] GSA initiated FedRAMP operations, which the agency referred to as initial operational capabilities, in June 2012.

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 formally established the FedRAMP program.[37] The act required OMB to:

- issue guidance defining the scope of FedRAMP and establish requirements for agencies to use it,

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

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

[37]*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, 3458 (Dec. 23, 2022), codified at 44 U.S.C. §§ 3607-16.

- create additional responsibilities for the FedRAMP Board and the GSA program management office, and
- establish a process to periodically review FedRAMP authorization packages to support the secure authorization and reuse of secure cloud products and services.

In response to the act, in July 2024, OMB issued its *Modernizing the Federal Risk and Authorization Management Program (FedRAMP)* guidance.[38] The guidance stated that the program would support the following paths for CSPs to obtain FedRAMP authorization to promote reusability while accommodating different use cases within the federal government:

- **Agency authorizations** are signed by the federal agency's authorizing official and indicate that an agency or a joint group of agencies assessed a CSP's security posture in accordance with FedRAMP guidelines and found it acceptable. The FedRAMP Director is responsible for ensuring that authorizations can reasonably support the presumption of adequacy. Authorizations can also be conducted jointly by multiple agencies to enable a cohort of agencies with similar needs to pool resources and achieve consensus on an acceptable risk posture for use of a cloud product or service.
- **Program authorizations** are signed by the FedRAMP Director and indicate that the program assessed a cloud service's security posture and found it met requirements and was acceptable for reuse by agency authorizing officials.
- **Other paths to authorization** are designed by the FedRAMP Program Management Office, in consultation with OMB and NIST, and approved by the FedRAMP Board to further promote the goals of the program. In all cases, any alternative pathways are to adhere to the rigorous standards of the program.
- **Time-specific temporary authorizations** allow federal agencies to pilot the use of new cloud services that do not yet have a full FedRAMP authorization. Consistent with FedRAMP's policies and procedures, such an authorization would serve as a temporary authorization. This type of authorization would provide for use of the covered product or service on

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

a trial basis for a specified period, not to exceed 12 months.[39] After 12 months, the temporary authorization would terminate, unless the CSP was in-progress for a full authorization.

OMB Guidance on Secure Software Development Practices for Cloud Products

Federal agencies are to use software provided by CSPs who can attest to complying with the government-specified secure software development practices, as described in NIST's *Secure Software Development Framework*.[40] This includes the software necessary for agencies to manage and provision cloud resources, as well as for SaaS applications, among other things. The guidance also states that agencies need to track and share all components of each software release using a software bill of materials (SBOM). Further, according to CISA, a SBOM should be machine-processable in a widely-used format and contain enough information about the open source and proprietary components in the software to correlate with other data sources, such as vulnerability databases and security advisories.[41]

According to NIST, an SBOM is a formal record containing the details and supply chain relationships of various components used in building software. Software developers and vendors often create products by assembling existing open source and commercial software components. The SBOM enumerates these components in a product.

In September 2022, OMB issued M-22-18, which was intended to help agencies ensure the integrity of their systems to protect against threats, vulnerabilities and cybersecurity risks.[42] The guidance outlined requirements for agency SBOM collection based on the criticality of the software. Agencies could consider information from SBOMs during the acquisition process and use them to manage vulnerabilities and licenses for software they had already acquired, which included cloud-related software.

[39]FedRAMP was to provide additional procedures related to this trial process, and agencies have been encouraged to coordinate with FedRAMP to ensure that there is no potential gap in service when the trial period concludes.

[40]National Institute of Standards and Technology, *Secure Software Development Framework*, Version 1.1 (2022).

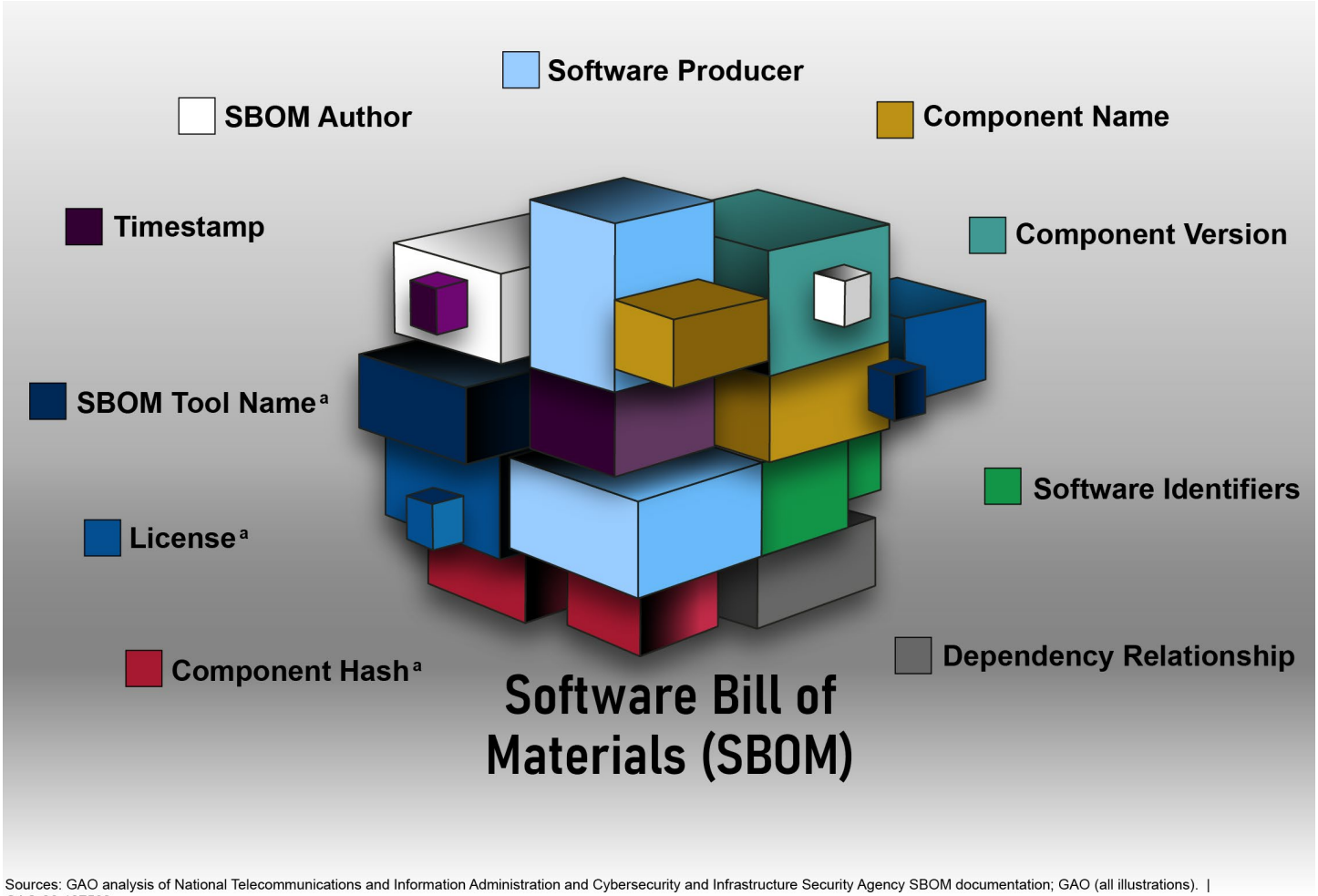
[41]Cybersecurity and Infrastructure Security Agency, *A Shared Vision of Software Bill of Materials (SBOM) for Cybersecurity* (Sept. 3, 2025).

[42]Office of Management and Budget, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*, M-22-18 (Washington, D.C.: Sept. 14, 2022).

Commerce's National Telecommunications and Information Administration, NIST, and CISA have issued guidance on what components should be included in an SBOM.[43] For example, in August 2025, CISA issued draft guidance updating the minimum elements for a bill of materials. The figure below illustrates the software components identified in federal guidance that comprise an SBOM.

[43]National Telecommunications and Information Administration, *The Minimum Elements for a Software Bill of Elements (SBOM), Pursuant to Executive Order 14028 on Improving the Nation's Cybersecurity* (July 12, 2021); National Institute of Standards and Technology, *Guidance on Supply Chain Security under EO 14028 Section 4c/4d* (May 5, 2022); and Cybersecurity and Infrastructure Security Agency, *2025 Minimum Software Bill of Materials (SBOM)*, Public Comment Draft (Aug. 2025).

Figure 4: Illustration of a Software Bill of Materials with the Software Components Identified in Federal Guidance



Sources: GAO analysis of National Telecommunications and Information Administration and Cybersecurity and Infrastructure Security Agency SBOM documentation; GAO (all illustrations). | GAO-26-107530

[a]New minimum elements for software bill of materials proposed by the Cybersecurity and Infrastructure Security Agency in August 2025.

OMB Guidance on Federal Cloud Procurement Data

Prior to February 24, 2026, the primary government-wide database for contracting information, including cloud contracts, within the federal government was FPDS.[44] The Administrator of OFPP established the database in 1978 and has been responsible for issuing FPDS guidance

[44]*Federal Funding Accountability and Transparency Act of 2006*, Pub. L. No. 109-282, 31 U.S.C § 6101 note (2006). See also FAR 4.603 (legacy).

and policy, including how data is collected and used.[45] GSA has administered the system on OFPP's behalf since 1982. Subsequently, on February 24, 2026, GSA retired the FPDS.gov website and its ezSearch tool, migrating federal procurement data into SAM.gov.[46] According to the SAM.gov website, it is now the centralized platform for contracting data within the federal government.

For more than a decade, OMB has worked to improve the quality of federal agency procurement data, including cloud procurement data, by issuing guidance and implementing key initiatives. In May 2011, OMB issued guidance that described the steps that federal agencies were to take to ensure that FPDS and other acquisition-related information, including cloud contracts, were accurately reported.[47] As part of the guidance, agency Chief Acquisition Officers were required to annually certify each January to OFPP that the agency's previous fiscal year's FPDS records were complete and accurate.[48]

In November 2023, the President announced the Better Contracting Initiative to ensure that the federal government was getting better terms and prices when purchasing goods and services, including cloud services. This included, among other things:

- **Leveraging data across federal agencies to get lower prices and better terms in areas such as cloud contracts.** OMB stated that limited

[45]Under the *Office of Federal Procurement Policy Act of 1974*, the Administrator of OFPP was required to establish a system for collecting and developing information about federal procurement contracts. *Office of Federal Procurement Policy Act of 1974*, Pub. L. No. 93-400 (1974).

[46]We have previously reported on GSA's efforts to consolidate government-wide acquisition data systems. See GAO, *Federal Spending Transparency: Actions Needed to Help Ensure Procurement Data Quality*, GAO-25-107469 (Washington: D.C.: Sept. 25, 2025) and *Federal Contracting: Effort to Consolidate Governmentwide Acquisition Data Systems Should Be Reassessed*, GAO-12-429 (Washington, D.C.: Mar. 15, 2012).

[47]Office of Management and Budget, *Improving Federal Procurement Data Quality – Guidance for Annual Verification and Validation* (Washington, D.C.: May 31, 2011).

[48]The relevant version of the FAR, for the purposes of this report, states that chief acquisition officers for each agency are required to report its contract actions to GSA, in accordance with FPDS guidance, within 120 days after the end of each fiscal year. Each agency must submit an annual certification of whether, and to what degree, agency Central Accounting Reporting System data for the preceding fiscal year is complete and accurate. FAR 4.604(c)(legacy). GSA officials reported that OMB manages the overall process, and GSA enters the overall completeness and accuracy measures of agency FPDS data into the system.

central capacity for analytics and insights had hindered the ability to compare prices and terms across agencies. To address this issue, OMB launched a centralized data management strategy, which created a Hi-Def framework for sharing and analyzing acquisition data, including cloud contract data, across the federal enterprise.[49] The intent of the Hi-Def Initiative, including the framework, was to enable agencies to more efficiently and effectively acquire products and services, including cloud services, as well as gain acquisition insights.

In June 2024, the Procurement Co-Pilot was launched, which was powered by Hi-Def strategic acquisition data. The pilot is a new government-wide acquisition market and price research tool to streamline the procurement process. The tool leverages data from FPDS, SAM,[50] transactional prices paid data from Best-in-Class contract vehicles, including cloud contract vehicles, and GSA's Transactional Data Reporting program.[51]

- **Negotiating common enterprise-wide software licenses in areas such as cloud SaaS licenses.** OMB noted that prices routinely vary up to 20 percent for the same software across agencies. GSA was to lead the government in negotiating government-wide IT software license agreements with large software providers. This change was intended to help to reduce price variance, secure more favorable terms and conditions, and avoid the wasted effort of having each agency individually plan, research and negotiate for the same common requirement.

  In May 2024, OMB issued Circular A-137, *Strategic Management of Acquisition Data and Information*, to improve agency access to reliable acquisition data and information, including cloud information.[52] Under

[49]The Hi-Def framework provides policies, data standards, and governance addressing the acquisition of supplies or services using relevant acquisition data that is easily accessed and consumed at the time of need. The framework promotes data interoperability, secure sharing of acquisition data between agencies, and enterprise-wide data analysis to inform government-wide and individual agency procurements.

[50]SAM.gov is the primary government repository for prospective federal awardee and federal awardee information.

[51]GSA's Transactional Data Reporting program collects data about the prices paid for products and services sold through GSA Multiple Award Schedule contracts to help understand what the government purchases. Data elements required to be reported for each transaction include product descriptions, quantities, and prices. GSA's Multiple Award Schedule program establishes government-wide contracts that provide access to more than 25 million commercial products and services.

[52]Office of Management and Budget, *Strategic Management of Acquisition Data and Information*, Circular A-137 (May 14, 2024).

Circular A-137, GSA will serve as the Managing Agency for the Hi-Def Environment. In addition, GSA has been assigned the responsibility for managing the technical architecture and planned capabilities for the environment.

Federal Cloud Contracting

Federal government spending on contracts for cloud services has grown rapidly over the past 10 years, from $2.3 billion to over $10 billion each year.[53] These contracts include a variety of cloud-related services, from virtual machines or database hosting to cloud-based storage, and application development and deployment. The government also uses a variety of SaaS applications, from word processing, grants management, continuous monitoring, and threat protection applications, to budgeting, licenses, and workforce applications.

As the office with primary responsibility for oversight of federal procurement, OFPP is responsible for providing direction for government-wide procurement policies to promote efficiency and effectiveness in government acquisitions, including cloud-related acquisitions. The Administrator for OFPP directs the development of these policies. Amendments and revisions to federal regulations are overseen by the FAR Council. The Revolutionary FAR Overhaul is ongoing. According to the overhaul website, Part 2 and Part 52 were released on October 28, 2025. which completed Phase One.[54] The overhaul is currently entering the next phase where federal rulemaking is intended to be conducted to permanently replace the legacy FAR text with the deviated language. Phase Two is intended to have a period for public comment.

Within each agency, contracting officers are responsible for ensuring performance of all necessary actions for effective cloud contracting, ensuring compliance with the terms of the contract, and safeguarding the interests of the United States in its contractual relationships.[55] Contracting officer's representatives assist in the technical monitoring or administration of the contract.[56] GSA outlined several acquisition stages that enable government agencies to procure goods and services

[53]Data was obtained from the Federal IT Dashboard and federal agencies. OMB's IT Dashboard is a public website that provides detailed information on IT investments at 26 federal agencies. See https://itdashboard.gov/.

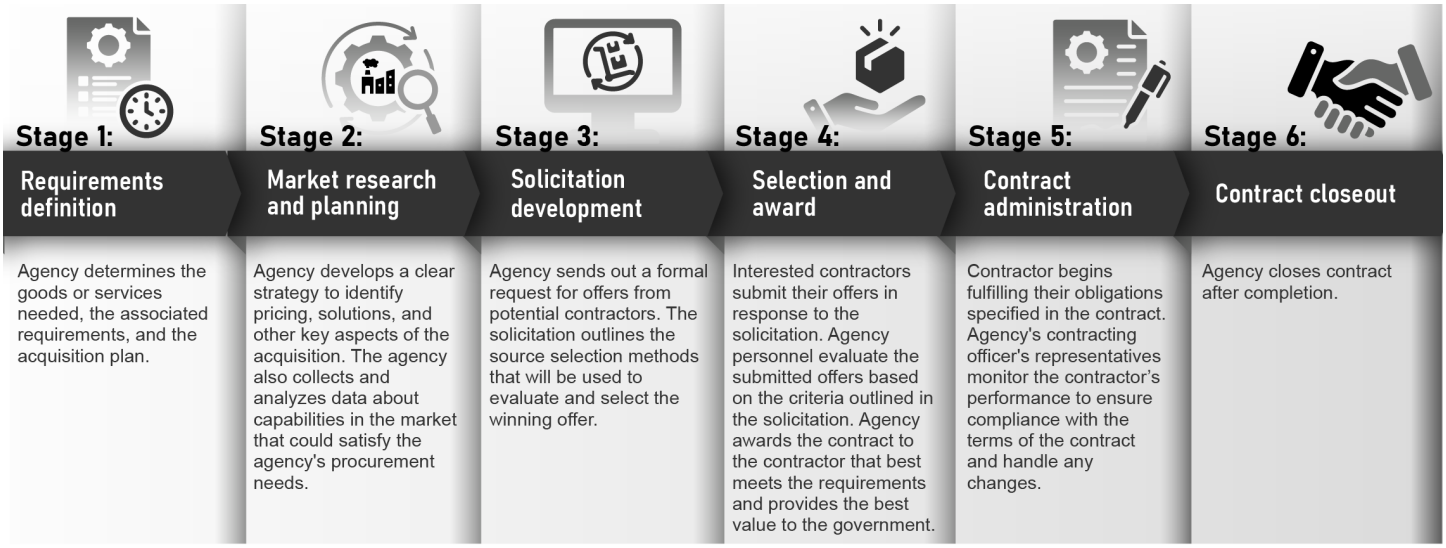
[54]"Revolutionary FAR Overhaul (RFO)", General Services Administration, last updated June 2, 2026, https://www.acquisition.gov/far-overhaul.

[55]FAR 1.602-2 (legacy).

[56]FAR 1.604 (legacy).

efficiently. Figure 5 provides a summary of the stages in a federal competitive acquisition process.

Figure 5: Stages in a Federal Competitive Acquisition Process



Sources: GAO analysis of General Services Administration federal acquisition stage documentation; Uniconlabs/stock.adobe.com (all icons). | GAO-26-107530

FAR Guidance on Cloud Computing Contracts

In 1979, Congress passed the Office of Federal Procurement Policy Act Amendments of 1979.[57] The law required OMB's Administrator of OFPP to develop a system of simplified and uniform procurement policies, procedures, and forms.

Subsequently, in April 1984, the FAR was established for the codification and publication of uniform policies and procedures for acquisition by executive agencies.[58] It is the primary regulation used by federal agencies to acquire products and services, including cloud services, with

[57]41 U.S.C. § 401 note.

[58]The Federal Aviation Administration, the U.S. Mint, mixed-ownership government corporations like the Federal Deposit Insurance Corporation and executive agencies that are funded with non-appropriated funds have been exempted from being subject to the FAR. *See Department of Transportation and Related Agencies Appropriations Act, 1996*, Pub. L. No. 104-50, § 348, 109 Stat. 460–61 (1995) (directing the Administrator of the Federal Aviation Administration to develop and implement an acquisition system for the agency). In addition, the FAR does not apply by law to agencies in the legislative and judicial branches of government although such agencies may choose to follow certain provisions of the FAR.

appropriated funds. This is intended to ensure fairness, transparency, and efficiency in government spending.

Specific parts of the FAR set policies and procedures to acquire commercial products and services, including cloud services.[59] The FAR's performance standards note that the government should maximize the use of commercial products and services, and that the regulatory system must perform in a timely, high quality, and cost-effective manner.[60]

Several parts of the FAR prescribe policy and procedures relevant to the acquisition and management of cloud computing contracts.

- Part 12 of the FAR prescribes policies and procedures related to the acquisition of commercial products and commercial services, including cloud services.
- Agencies may use firm-fixed-price contracts for the acquisition of commercial products or commercial services.[61] Agencies can use time-and-materials contracts or labor-hours contracts to acquire commercial services under certain conditions.[62]

Further, GSA has been given the authority to establish the Federal Supply Schedule, which provides federal agencies with a simplified process for obtaining commercial products and commercial services at prices associated with volume buying. In December 2021, GSA's Senior

[59]FAR Part 12 has undergone revision as part of the Revolutionary FAR Overhaul. Much of what was removed from the FAR, has been moved into practitioner albums, the *FAR Companion Version 2.0*, and other guides, which offer tools and guidance for everyday acquisition activities.

[60]FAR 1.102-2 (legacy). See also Executive Order 14271, *Ensuring Commercial, Cost-Effective Solutions in Federal Contracts*, directing that agencies procure commercially available products and services to the maximum extent practicable. Exec. Order No. 14271, 90 Fed. Reg. 16433 (Apr. 15, 2025). In addition, Executive Order, *Eliminating Waste and Saving Taxpayer Dollars by Consolidating Procurement*, directed the consolidation of domestic federal procurement under GSA and designated GSA as executive agent for all government-wide contracts for IT. Exec. Order No. 14240, 90 Fed. Reg. 13671 (Mar. 20, 2025).

[61]See FAR 16.203-2 (legacy) for the circumstances with fixed-price contracts with economic price adjustments may be used. The FAR 16.203-2 (deviation) continues to contain guidance on economical price adjustments.

[62]The FAR states that time-and-materials contracts may be used only when it is not possible, at the time of awarding the contract, to estimate accurately the extent or duration of the work or to anticipate costs with any reasonable degree of confidence. FAR 16.601(c) (legacy). The FAR 16.601 (deviation) continues to contain guidance on time-and-materials contracts.

Procurement Executive issued Acquisition Letter MV-21-06 to GSA's acquisition workforce. This letter established special ordering procedures for buying commercial cloud computing services on a consumption basis under the Federal Supply Schedule.[63] Subsequently, in March 2024, the GSA Senior Procurement Executive issued Acquisition Letter MV-2024-01 to provide guidance to contracting officers about purchasing cloud-based SaaS products.[64]

GAO Previously Reported on Federal Cloud Implementation and Private Sector Cloud Use

For more than a decade, we have reported on federal agencies' efforts to implement cloud services and the challenges they have identified with these efforts. In addition, we recently issued a report on private sector companies' use of cloud services.

In July 2012, we reported that seven federal agencies' (Agriculture, DHS, GSA, HHS, SBA, State, and the Treasury) efforts to implement cloud services could benefit from additional planning.[65] Specifically, to advance cloud adoption, federal agencies were required to select three IT services to migrate to the cloud and outline a plan that included costs, major milestones, and performance goals. Nineteen of the 20 plans we reviewed were missing one or more required elements. Accordingly, we recommended that the heads of the seven agencies take action to direct their CIOs to establish plans for legacy systems and other planned additional cloud-based services that included costs, performance goals, and plans. Six of the seven agencies implemented the recommendations. According to Treasury officials, they did not implement the recommendation on developing plans for legacy systems because the department had already implemented cloud-based services prior to the issuance of OMB's guidance.

In September 2014, we reviewed the efforts of the same seven federal agencies.[66] We found that the agencies had not assessed about 67

[63]General Services Administration Office of Governmentwide Policy, *Procurement of Cloud Computing on a Consumption Basis under the Federal Supply Schedule Program*, MV-21-06 (Washington, D.C.: Dec. 16, 2021).

[64]General Services Administration Office of Governmentwide Policy, *Guidance on Payment for Software Licenses Delivered via SaaS*, MV-2024-01 (Washington, D.C.: Mar. 15, 2024).

[65]GAO, *Information Technology Reform: Progress Made but Future Cloud Computing Efforts Should be Better Planned,* GAO-12-756 (Washington, D.C.: July 11, 2012).

[66]GAO, *Cloud Computing: Additional Opportunities and Savings Need to Be Pursued*, GAO-14-753 (Washington, D.C.: Sept. 25, 2014).

percent of their investments for cloud services, despite being required to do so by OMB.[67] We therefore recommended that the heads of the agencies direct their CIOs to ensure all IT investments within the agency were assessed for cloud services, including dates for investments that had not yet been assessed. Six of the seven agencies implemented the recommendations. Treasury officials reported that the department did not implement the recommendation because cloud assessments were only conducted if the department determined that an investment would be replaced, redeveloped, or retired.

In April 2016, we identified 10 key practices that federal and private-sector guidance noted should be included in service level agreements in a contract when acquiring IT services through a CSP.[68] Our review of five agencies' (Defense, DHS, HHS, Treasury, and VA) cloud service contracts found that not all 10 key practices were included in these contracts. We therefore made recommendations to OMB to include all 10 key practices in future guidance to agencies.

OMB took action to implement our recommendations. Specifically, in June 2019, OMB issued its Federal Cloud Computing Strategy. The strategy incorporated key practices on service level agreements and roles and responsibilities for the agency and the CSP. Subsequently, in January 2020, OMB staff reported that they had worked with GSA to identify service level agreement best practices and had made this guidance available to agencies through the Max.gov portal to help improve federal acquisition of cloud-based technologies.[69]

In April 2019, we found that 16 agencies we reviewed had made progress in implementing cloud computing services—namely, they established assessment guidance, performed assessments, and implemented these services—but the extent of agency progress varied.[70] In addition, the 16

[67]Starting in fiscal year 2014, OMB required agencies to evaluate each investment, or components or systems within the investment, for cloud services, regardless of the overall life-cycle stage of the investment. Office of Management and Budget, *FY 2014 Guidance on Exhibits 53 and 300* (Washington, D.C.: Aug. 3, 2012).

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

[69]In October 2023, OMB staff reported that OMB no longer provided guidance to agencies related to service level agreements on the MAX.gov portal.

[70]GAO, *Cloud Computing: Agencies Have Increased Usage and Realized Benefits, but Cost and Savings Data Need to be Better Tracked*, GAO-19-58 (Washington, D.C.: Apr. 4, 2019).

agencies reported that they had increased their cloud service spending since 2015. Thirteen of the 16 agencies had saved $291 million by 2019 from these services. However, these agencies identified issues in tracking and reporting cloud spending and savings data, including not having consistent processes in place to do so.

We therefore made recommendations to OMB to require agencies to report, at least on a quarterly basis, the savings and cost avoidance associated with cloud computing investments. In addition, we made recommendations to all 16 agencies to establish a consistent and repeatable mechanism to track savings and cost avoidances from the migration and deployment of cloud services. Fourteen of the 16 agencies (all but DOD and Transportation) have implemented our recommendation. As of March 2024, an official from OMB reported that it did not intend to take action to implement the recommendation. However, GAO continues to believe that agency reporting, at least quarterly, on the savings and cost avoidance from cloud computing investments is necessary. This will help to strengthen agency reporting on cloud savings data so that OMB and Congress have sufficient data to see the results of key initiatives like Cloud Smart. It will also help OMB and Congress to understand whether agencies are achieving savings using cloud services.

In December 2019, we reported that, while all 24 major federal agencies were participating in FedRAMP, many of these agencies continued to use cloud services that were not authorized through the program.[71] Further, we reported that although OMB required agencies to use the program, it did not effectively monitor agencies' compliance with this requirement. We therefore recommended, among other things, that OMB establish a process for monitoring and holding agencies accountable for authorizing cloud services through FedRAMP.

OMB has implemented our recommendation. Specifically, OMB issued memorandum M-24-15, *Modernizing the Federal Risk and Authorization Management Program (FedRAMP)*. This guidance requires agencies to provide a copy of authorization letters and any relevant supplementary information to the FedRAMP program management office.

In January 2024, we reported that data on the actual costs of FedRAMP authorization were limited, although selected agencies and CSPs

[71]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).

provided estimated costs.[72] In addition, the estimated costs varied widely and ranged anywhere from tens of thousands to millions of dollars. This was due, in part, to the agencies and the providers using varying methods to determine costs.

We therefore made a recommendation to OMB, in collaboration with the FedRAMP Program Management Office, to issue guidance to agencies to ensure that the agencies consistently track and report the costs of sponsoring a FedRAMP authorization of cloud services. OMB took action to implement our recommendation in July 2024 by issuing M-24-15. This guidance stated that agencies must report the costs of pursuing FedRAMP authorizations.[73]

In September 2024, we reported that agencies had mixed results in setting policies and guidance that addressed the five key cloud procurement requirements established by OMB in its 2019 Cloud Smart Strategy.[74] Most agencies did not establish service level agreement guidance, which define the levels of service and performance that the agency expects its cloud providers to meet. In addition, nearly one-third of agencies did not have guidance to ensure continuous visibility in high value assets (systems that process high-value information or serve a critical function in maintaining the security of the civilian enterprise).

Consequently, we made 46 recommendations to 18 agencies to develop or update guidance associated with OMB's Cloud Smart procurement requirements. Fourteen agencies agreed with all recommendations, one agency did not explicitly agree but provided planned actions, three agencies neither agreed nor disagreed, and one (Department of Education) disagreed. As of June 2026, seven agencies (Agriculture, Commerce, Education, Labor, GSA, SSA, and USAID) had implemented our recommendations. In addition, we had previously made a recommendation to Treasury related to establishing guidance on SLAs.[75] Treasury had also implemented this recommendation as of May 2026.

[72]GAO, *Federal Authorization Program Usage Increasing, but Challenges Need to Be Fully Addressed*, GAO-24-106591 (Washington, D.C.: Jan. 18, 2024).

[73]Office of Management and Budget, *Modernizing the Federal Risk and Authorization Management Program (FedRAMP)*.

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

[75]GAO-16-325.

We also made one recommendation to the CIO Council to collect and share examples of agency guidance and contract language on OMB's requirements in the Federal Cloud Computing Strategy. The Council neither agreed nor disagreed with our recommendation and has not yet implemented it.

In March 2025, we reported that 18 surveyed private sector companies stated they were using the majority of 19 leading cloud computing practices across three management areas—acquisition, cybersecurity, and workforce development.[76] Subject matter experts from academia agreed these were leading practices for cloud adoption, and the majority of companies found them very or extremely important for an effective cloud adoption strategy. Included among the practices were that organizations should evaluate their retention and recruiting strategies to identify and address skill gaps.

Agencies and OMB Used Imprecise Cloud Procurement Data

Agencies mainly used historical data to make cloud procurement decisions. However, the agency-reported obligations on cloud contracts in FPDS were imprecise due to how IT-related product and service codes (PSC) are assigned to contracts in this system. Issues with having reliable data in FPDS are not new and we have made numerous recommendations to address them.

Agencies and OMB Primarily Used Historical Data to Help Make Decisions

All 24 agencies used cloud-related data to guide decision-making regarding cloud procurements. Most of the agencies used historical procurement data. Specifically, senior officials from the Offices of the CIO and Senior Procurement Executive or Chief Acquisition Officer from 22 of the 24 agencies reported that the agencies relied on historical procurement and contract data to provide insights into current and future investments. This included a wide range of data on each contract (e.g., contract type, periods of performance, issue date), spending history, requirements, vendor performance, service level agreement conformance, and FedRAMP information. For example:

- Commerce officials stated that the agency's use of budget, IT, and acquisition data helped inform the agency's IT modernization efforts because it enabled agency officials to consider each investment's total

[76]GAO, *Cloud Computing: Private Sector Leading Practices in Acquisition, Cybersecurity, and Workforce Development,* GAO-25-106369 (Washington, D.C.: Mar. 24, 2025).

cost of ownership when determining whether to move investments to cloud services.[77]

- Justice officials reported that the agency's data collection helped the agency determine, among other things, which providers the components were working with, and the volume and percentage of services being procured. Officials said this information also helped the agency understand where it was making its investments in these services. The officials added that the agency used this information to identify opportunities for cloud enterprise license agreements. The officials stated that it was important to collaborate with components that had been early procurers of cloud services because the component's information was key in helping make decisions agency-wide.
- Interior officials said that the agency used the data to track how each cloud investment fit into the agency's portfolio. The officials said that this informed the agency whether there were investments that needed to be addressed, and the agency could make decisions based on what percentage of the IT portfolio was being spent on certain functions.

In addition, officials from seven of the 24 agencies said that the agencies conducted market research on cloud computing services as part of the procurement process.[78] For example, NSF officials said that the agency had conducted market research to identify cloud vendors that could provide services that the agency would need with its current architecture. According to USAID officials, the agency conducted market research mainly to obtain pricing information and other benchmark data on cloud services. SSA officials stated that the agency conducted market research

[77]Total cost of ownership is generally calculated by determining the product or service's implementation and operational costs as well as related costs. These related costs include, among other things, overhead, salaries, technology upgrades, software support, and maintenance.

[78]The FAR previously defined market research as the process used to collect and analyze data about capabilities in the market that could satisfy an agency's procurement needs. FAR 10.002(b)(1)(legacy). Much of FAR Part 10 was moved into the *FAR Companion Version 2.0*, which provides general policies and procedures for conducting market research. The FAR Companion now directs federal acquisition teams to approach market research as an incremental process that build understanding step by step. If the agency is unable to fulfill the need, the next phase of market research focuses on whether shared services and other existing federal contract vehicles already offer the products or services needed. If existing contracts do not meet the requirements, then the agency is to assess the marketplace more broadly for open market acquisition. See FAR Companion 2.0 10.001. The FAR Council developed the *FAR Companion Version 2.0* to help acquisition officials exercise their discretion. The companion guidance provides context, additional information, and practical advice for planning, awarding, managing, and closing out contracts, consistent with the FAR's core buying principles. Federal Acquisition Regulatory Council*, FAR Companion (FC), Version 2.0* (October 30, 2025).

to identify projected consumption pricing, historical data on cloud usage, and potential discounts based on volume.

Further, OMB used several sources of agency-provided cloud procurement data to guide decision-making regarding cloud initiatives. This included cloud procurement data, data on authorized federal cloud providers, and the cloud services that agencies used.[79] OMB staff from the Office of the Federal CIO stated that they used the cloud procurement data collected to make decisions regarding the development of government-wide strategies and policies regarding cloud technology.

Finally, the staff stated that they used the data collected to coordinate with federal agencies on cloud implementation, including procurement of these services. OMB staff stated that the office also coordinated with several offices within GSA, including the IT Vendor Management Office, which works to improve how the government buys common IT goods and services. For example:

- **Agency cloud contract data.** OMB staff reported that OMB collected cloud contract data from FPDS, the primary federal database for contracting information, to assist with decisions regarding procurement policy.[80] OMB staff noted that OMB had been working to modernize IT-related PSCs, particularly cloud services, to identify how much the federal government was spending. The PSCs were updated in October 2020, replacing one code for cloud computing with eight cloud-related

[79]OMB previously collected additional data on cloud spending from the agencies. In 2012, OMB began requiring agencies to report associated cloud spending, as called for in its annual capital planning guidance. For fiscal years 2015 through 2018, OMB's capital planning guidance required agencies to report their total cloud spending at the agency level based on the cloud deployment model, rather than by individual investment. Starting in fiscal year 2019, OMB required agencies to report total cloud spending by investment. In 2021, OMB discontinued the reporting of cloud spending in its annual guidance to agencies for fiscal year 2023.

[80]Prior to February 24, 2026, FPDS provided a comprehensive web-based tool for agencies to report contract actions. Executive agencies were to use FPDS to maintain publicly available information about all unclassified contract actions (exceeding the micro-purchase threshold) and any modifications to those actions that change previously reported contract action report data, regardless of dollar value. Following GSA's retirement of the FPDS.gov website on February 24, 2026, agencies will provide their contract data through the contract award management web portal on SAM.gov.

codes.[81] This included additional codes for products purchased by the government (i.e., hardware and software), capability delivered "as a service" (cloud computing), and support services (e.g., virtual server support and continuous monitoring). This was intended to allow agencies to capture and report more granular cost data.

- **Authorized federal cloud providers**. OMB staff relied on information from the FedRAMP Marketplace to determine which CSPs were authorized.[82]
- **Types of cloud services used by agencies.** OMB staff reported that OMB collected data on agency use of cloud services and providers as part of the annual Federal Information Security Modernization Act metrics, including whether the agency used an authorized provider.[83]

Obligations on Cloud Contract Data in FPDS Were Imprecise

Federal agency cloud contract obligation data in FPDS were imprecise due to how PSCs are assigned to contracts in the system.[84] OFPP requires that one principal (or predominant) PSC is assigned to each

[81]The new cloud-related codes included: (1) business application and application development software as a service (DA10), (2) compute as a service (DB10), (3) data center as a service (DC10), (4) end user as a service (DE10), (5) IT management as a service (DF10), (6) network as a service (DG10), (7) platform as a service (DH10), and (8) storage as a service (DK10). For more details on the PSCs, see appendix I.

[82]According to FedRAMP's program management office, the FedRAMP Marketplace is a publicly available website that provides a database listing of cloud service offerings to help agencies research and identify secure cloud services that are available for government-wide use.

[83]The *Federal Information Security Modernization Act* requires agency CIOs to submit reports on their agency's information security programs to OMB, DHS, GAO, and Congress. 44 U.S.C. § 3553 (*Federal Information Security Modernization Act of 2014).* OMB and CISA collaborate with interagency partners to develop the CIO Federal Information Security Modernization Act metrics. OMB calls for agencies to provide this information on a quarterly basis.

[84]We assessed the reliability of the FPDS cloud contract data because OMB stated that it used these data to make decisions regarding cloud procurements. Further details on our methodology for this assessment are included in appendix I.

contract.[85] Multiple codes are not allowed to be assigned—even if services other than cloud are being purchased.

Senior agency officials reported that this impacted their reporting of obligations on contracts for cloud computing in FPDS. Specifically, senior officials in the Offices of the CIO and Senior Procurement Executive or Chief Acquisition Officer from 13 agencies reported that they had contracts in place where: (1) the PSC reflected a service other than cloud because cloud services was a secondary purchase and (2) a cloud code was assigned but services besides cloud were also being acquired.

As a result, we found that FPDS data could not be used to determine precise agency obligations on contracts for cloud services. If other, non-predominant services were included in a contract with a cloud PSC, the data would reflect obligations for these in addition to cloud services. In addition, the obligations on contracts where cloud services were not predominant, would not include cloud-related PSCs.

Officials at nine agencies in our review also expressed concerns about OMB using FPDS as a primary source for obligations on contracts for cloud services. These officials noted that the agencies maintained better data on cloud spending than the data in FPDS.[86] Some agency officials noted that their federal agency contract writing systems were able to input multiple PSCs using XML templates. Other officials reported that only one PSC was captured in their internal systems because of OFPP's FPDS-related requirement. OMB staff acknowledged that, by using PSCs based

[85]According to the FPDS Product and Service Codes Manual, a given contract may include more than one product or service. In such cases, the product or service code should be selected based on the predominant product or service that is being purchased. General Services Administration, *Federal Procurement Data System Product and Service Codes Manual Fiscal Year 2021 Edition* (Washington, D.C.: October 2020). Subsequently, in April 2025, GSA issued another version of the manual. We reviewed the 2025 version of the manual and confirmed that the same language regarding product or service codes was included in this version of the manual. See General Services Administration, *Federal Procurement Data System Product and Service Codes Manual Fiscal Year 2025 Edition* (Washington, D.C.: April 2025).

[86]Agency contract data is typically maintained in agency contracting systems, such as contract writing systems or other contract management systems. Prior to February 24, 2026, agencies accessed FPDS through the system's website (https://www.fpds.gov) to report their contract data or configure their contract writing system(s) to interface with the procurement system for reporting. Following the retirement of the FPDS.gov website on February 24, 2026, agency contract writing systems will provide their contract data through the contract award management web portal on SAM.gov.

on the preponderance of the contract value, FPDS would not accurately capture all or only cloud-based spending.

Subsequently, on February 24, 2026, GSA retired the FPDS.gov website and its ezSearch tool, migrating federal procurement data into SAM.gov. According to the SAM.gov website, it now is the centralized platform for contracting data in the federal government. Although GSA made changes to SAM.gov as part of the migration effort, including requiring user confirmation of data accuracy before final submission, no changes to the PSC fields were made.

Challenges with federal procurement data are not new. Since its creation more than 40 years ago, FPDS has had a history of data completeness and accuracy challenges. For example, in 1980, we reported on known procurement system errors and in 1994 we determined that the system was not subject to standards on the appropriate levels of accuracy and completeness.[87] In 2003, we reported serious and continuing concerns with the reliability of the system's data.[88] We found that FPDS data were either understated or overstated by millions of dollars and that the value of contracts had been hundreds of millions of dollars different than reported. We pointed out that Congress and executive branch agencies relied on these data to assess the impact of government-wide acquisition policies.

OMB took significant action to address these continuing data reliability challenges by issuing FPDS guidance in 2007, 2008, 2009, and 2011.[89] Primarily, the guidance required federal agencies to complete an annual

[87]U.S. General Accounting Office, *The Federal Procurement Data System—Making It Work Better*, GAO/PSAD-80-33 (Washington, D.C.: Apr. 18, 1980); and *OMB and GSA: FPDS Improvements*, GAO/AIMD-94-178R (Washington, D.C.: Aug. 19, 1994).

[88]GAO, *Contract Management: No Reliable Data to Measure Benefits of the Simplified Acquisition Test Program*, GAO-03-1068 (Washington, D.C.: Sept. 30, 2003).

[89]Office of Management and Budget, *Improving Federal Procurement Data Quality - Guidance for Annual Verification and Validation* (Washington, D.C.: May 31, 2011); *Improving Acquisition Data Quality for Fiscal Years 2009 and 2010* (Washington, D.C.: Oct. 7, 2009); *Improving Acquisition Data Quality—FY 2008 FPDS Data* (Washington, D.C.: May 9, 2008); and *Federal Procurement Data Verification and Validation* (Washington, D.C.: Mar. 9, 2007). According to OMB, the 2007 memorandum was rescinded by the 2008 memorandum, and the 2008, 2009, and 2011 memorandums remain in effect unless a subsequent version specifically addresses, rescinds, or supersedes a prior version.

verification and validation process and certify the data submitted to FPDS were complete, accurate, and timely.

However, we reported in September 2025 that almost half of the agencies we reviewed did not complete the data quality report in fiscal year 2023.[90] Specifically, of the 70 federal agencies reporting data for fiscal year 2023, 23 agencies did not complete the required report and 11 did not respond to our requests for copies of their reports.[91] Further, none of the procurement data quality reports for the 24 agencies in our review fully met OMB's reporting requirements for fiscal year 2023.[92] To help ensure procurement data quality, we made a total of 12 recommendations to OMB, GSA, and four other selected agencies. GSA and the four agencies concurred with our recommendations; OMB did not provide comments on the report.

We have made numerous recommendations to federal agencies to address FPDS data quality. To their credit, most agencies took action to implement the recommendations. Continuing to implement those open recommendations at federal agencies can help to ensure quality information.

Agencies Reported Governance, Contracting, and Training Practices Assisted Cloud Procurements

Federal agencies managed and oversaw agency cloud procurement efforts by implementing practices in three areas.[93] Specifically,

- 21 agencies reported that putting governance structures, processes, and documentation in place assisted agencies in providing management and oversight of cloud procurement services;
- 18 agencies identified contracting approaches they used to facilitate procurement of cloud services; and

[90]GAO, *Federal Spending Transparency: Actions Needed to Help Ensure Procurement Data Quality*, GAO-25-107469 (Washington, D.C.: Sept. 25, 2025).

[91]These 34 agencies accounted for almost $2 billion, or about 0.26 percent, of the $759.2 billion in contract obligations reported to FPDS for fiscal year 2023.

[92]The 24 agencies accounted for over 99 percent of the $759.2 billion in contract obligations reported to FPDS for fiscal year 2023.

[93]We developed the list of three practices by reviewing interview responses, agency-provided cloud policies, guidance, and other process documentation; federal leading practice guidance; and prior related reports. All the 24 agencies had at least one or more of these practices in place.

- 8 agencies reported that they provided a variety of training opportunities with the goal of enhancing the staff's expertise in cloud acquisitions.

Governance Among Stakeholders Facilitated Management and Oversight of Cloud Procurements

Having governance structures, processes, and documentation assisted federal agencies in providing management and oversight of cloud procurement services. Senior officials from 21 of the 24 agencies reported that putting these processes in place helped their agencies to ensure the management and oversight of these services. These officials discussed the following types of governance that assisted their agencies.

Fifteen of the 21 agencies established offices that had primary responsibility for the procurement of cloud computing services within the agency. Three of the 15 agencies had offices that focused only on agency-wide cloud procurements. The remaining six of the 21 agencies had bureaus and program offices that generally had responsibility for cloud procurement.

Of the 15 agencies with a centralized office, six agencies reported that their offices were under the Senior Procurement Executive or Chief Acquisition Officer, five were under the Office of the CIO, three were under another organization, and one was managed jointly by the Office of the CIO and Senior Procurement Executive. For example, SSA officials reported that cloud procurement was the responsibility of the Senior Procurement Executive's Office of IT Acquisition and Grants. SBA officials reported that the Office of the CIO was responsible for cloud procurement at the agency. Transportation officials reported that they had established an IT Acquisition Center of Excellence, which procured and managed the agency's cloud acquisitions and contracts. Transportation officials noted that the center also reviewed agency data, including IT costs and spend plans, for additional opportunities to transition IT resources to enterprise solutions to improve efficiency.

Of the six agencies that reported that bureaus and program offices had responsibility for procurement, five agencies reported having additional enterprise governance in place. For example, two agencies reported that, while the offices did their own procurements, the agency CIO had to approve the procurement. Other agencies reported that offices were required to choose from a catalog of cloud services or use a FedRAMP-authorized cloud provider. In addition, although DOD did not have an agency-wide office, DOD officials reported that each of the military services within the agency had stood up its own cloud management office. These officials added that it allowed the services to centralize subject matter expertise and best practices to optimize delivery in terms

of performance and cost, get better visibility of those costs, and provide better risk management and security.

In addition, officials from 17 of the 21 agencies reported utilizing cloud working groups, communities of practice, technical boards or committees as part of the agency's governance activities. For example:

- Agriculture established an internal cloud working group to apply lessons learned across the agency, according to the group's charter. The group developed guidance on all aspects of cloud services enterprise-wide including purchasing, implementation, management, data integration, and operational optimization.
- DOD established a software modernization steering group, which led the implementation of the agency's software modernization activities.[94] The steering group's strategy indicated that it was responsible for supporting the agency's strategy to accelerate the DOD enterprise cloud environment using a multi-cloud, multi-vendor approach as the foundation for software modernization.
- Interior and VA established technical review boards, which helped their procurement offices assess planned procurement efforts. Interior's Technical Readiness Board charter stated that the board was focused on conducting initial technical assessments prior to agency cloud purchases.

All 21 agencies provided documentation that described how the agency ensured management and oversight of its cloud procurements. These processes were generally in three areas:

- **Reviews of cloud procurements using portfolio review and IT acquisition review boards.** Seventeen agencies used review boards as part of the procurement process. For example, EPA officials reported that the agency conducted reviews of cloud procurements through its Federal Information Technology Acquisition Reform Act (FITARA) review and IT portfolio review processes.[95] EPA officials reported that these reviews had identified opportunities to centralize cloud-based software licensing or reduce or centralize the licensing of applications. DHS officials reported that all of the agency's cloud procurements went through the agency's investment technology acquisition review process. The officials

[94]Department of Defense, *Department of Defense Software Modernization Strategy* (Feb. 2, 2022).

[95]*Carl Levin and Howard P. 'Buck' McKeon National Defense Authorization Act for Fiscal Year 2015*, Pub. L. No. 113-291, division A, title VIII, subtitle D, 128 Stat. 3292, 3438-50 (Dec. 19, 2014). 40 U.S.C. § 11319.

said that it provided an opportunity under FITARA for the component CIO, subject matter experts, lines of business, and other stakeholders to ensure that the procurement aligned to the enterprise architecture and agency IT strategy.[96]

- **Approvals required for cloud services by entity within the agency.** Four agencies reported that they required offices to seek approval for cloud procurements from specific entities within the agencies. For example, NSF officials reported that all new cloud service requests had to be submitted to the Division of Information Systems' Change Control Board and Engineering Review Board. The officials said it was to ensure that the planned approach for the use of cloud services aligned with agency and federal requirements pertaining to infrastructure, architecture, web services, and data management. OPM officials reported that all cloud procurements with a specific dollar threshold needed to seek approval of OPM's Capital Investment Committee. Interior officials reported that offices had to submit a request form to the Office of the CIO for cloud services managed by the agency and to the Technical Review Board for outside services.
- **Collaborations with stakeholders in other offices in the agency.** Officials from the Offices of the CIO at nine agencies noted that they had collaborated with the Offices of the Chief Acquisition Officer or Senior Procurement Executive, Offices of General Counsel, and other offices within the agencies on cloud procurements.[97] For example, senior officials from Energy reported that effective collaboration between the Office of the CIO and Acquisition Management enabled the offices to work together to determine what needed to be procured across the agency. Similarly, senior officials from Labor reported that procurement officials and the Office of the CIO collaborated on every procurement, and throughout the agency's advanced acquisition process.

  SSA senior officials reported that continuous coordination was required between the Offices of the Chief Financial Officer, the CIO, the Senior Procurement Executive, and the Office of General Counsel. Education

[96]As part of the President's Management Agenda, OMB created the lines of business initiative in March 2004. The initiatives were to address redundant IT investments and business processes across the federal government including case management, grants management, human resources management, federal health architecture, information systems security, budget formulation and execution, geospatial, and IT infrastructure.

[97]A Chief Acquisition Officer advises and assists agency leadership to help ensure that the agency's mission is achieved through the management of its acquisition activities. 41. U.S.C. § 1702(a). A Senior Procurement Executive is responsible for management direction of the agency's procurement system, including implementation of the agency's unique procurement policies, regulations, and standards. 41 U.S.C. § 1702(c).

officials reported that acquisition staff worked closely with staff from the Office of General Counsel, and the Office of Planning, Evaluation, and Policy Development's Governance and Strategy Division.

Agencies Identified Contracting Approaches Used to Facilitate Procurement of Cloud Services

Eighteen agencies identified contracting approaches they used to facilitate procurement of cloud services.[98] Specifically, officials from 15 of the 18 agencies reported that they had worked to optimize their cloud contract management approaches to improve cloud provider service. For example, some agencies consolidated cloud services into centralized enterprise cloud environments to reduce the need for numerous contracts. Other agencies focused on facilitating access with multiple cloud providers to obtain the benefits associated with a multi-cloud environment. In addition, several agencies procured cloud services through third-party vendors or resellers to obtain additional support, cost savings, and flexibility rather than directly with CSPs. Specifically:

- Senior officials from five agencies reported benefits from centralizing enterprise-wide cloud environments for all or part of the agencies.[99] DOD's enterprise-wide acquisition vehicle enabled the agency to acquire commercial cloud services directly from four CSPs. DOD officials said the benefits of centralization included building out a common infrastructure, improving incident response and vendor management for cybersecurity, and avoiding vendor lock-in. VA also acquired a multi-cloud environment using centralized contracts with two CSPs. VA's documentation indicated that having this enterprise cloud environment allowed developers to focus on delivering functionality rather than infrastructure management.
- Eight agencies supported cloud environments with multiple cloud providers.[100] For example, Treasury officials reported that the agency now used a single third-party vendor contract to facilitate access to multiple cloud providers. HHS reported leveraging its blanket purchase

[98]Acquisition planning by each agency may be impacted depending on how GSA implements the consolidation effort.

[99]GSA's *Cloud Contracting Quick Reference Guide* states that, whenever possible, contracting for IaaS cloud services should be done at the enterprise level to maintain the most control and the most consistent pricing across all constituent groups. See General Services Administration Office of Government-wide Policy, *Cloud Contracting Quick Referencing Guide* (November 2023).

[100]GSA's *Cloud Contracting Quick Reference Guide* notes that the benefits of a multi-cloud approach include expanded cloud options, increased competition, and reduction of vendor lock-in.

agreement with two cloud providers to drive competition between the vendors for the agency's benefit.

- Senior officials from five agencies reported obtaining better discounts from third-party vendors and resellers instead of CSPs.[101] For example, SBA senior officials noted that resellers provided benefits like increased discounts; cloud resource reservation through partner programs; and discounted access to specialists, support, and training. Senior NASA officials stated that this approach provided on-demand acquisition capabilities and offered the flexibility to leverage a multi-cloud strategy based on technical requirements.

Agencies Identified Pre-award Activities to Facilitate Contract Development

Sixteen of the 18 agencies reported taking pre-award actions that helped the agency to support contract development for cloud services. Specifically:

- Based on agencies' procurement policy documentation, 12 of the 16 agencies leveraged GWACs that OMB had designated as Best-in-Class to improve the acquisition of cloud services.[102] For example, officials from SSA stated that the benefits of the blanket purchase agreement that they used included contract terms such as fixed prices for cloud services, a percentage discount on these services, and a discount each option year in the contract. Treasury officials described plans to move to a Best-in-Class vehicle for managed cloud services to have better control over cloud spending, improve the security of its investments, and leverage the buying power of the agency.
- Senior officials from six of the 16 agencies stated that the agencies had developed catalogs of approved cloud services to reduce the time spent performing market research on cloud solutions. According to agency cloud policy documentation, four of the six agencies required cloud services to be limited to only those vetted solutions listed in the catalog. For example, State established a catalog of services from its central

[101]Cloud resellers (or cloud brokers) typically procure cloud services from CSPs and resell them to their own customers along with value-added services to help customers manage and operate cloud systems.

[102]The Best-in-Class designation identifies government-wide contracts that can be used by multiple agencies and that satisfy key OMB-defined criteria. The criteria include having rigorous requirements definitions and planning processes, appropriate pricing strategies, and data to measure performance. Agencies in our review that operated Best-in-Class GWACs that procured cloud services as of March 2025 included HHS's National Institutes of Health, GSA, and NASA. Under Executive Order 14240, *Eliminating Waste and Saving Taxpayer Dollars by Consolidating Procurement,* GSA will assume control of the Best-in-Class contracts from the agencies. Exec. Order No. 14240, 90 Fed. Reg. 13671 (Mar. 20, 2025).

cloud contract to make ordering cloud services easier and to obtain economies of scale and discounts. HUD's guidance also required components to obtain CIO approval to procure services from its catalog. Interior and Treasury's guidance indicated that the agencies did not require cloud procurements to use their agency's catalogs of CSPs, if doing so met the agency's requirements.

- Senior officials from four agencies reported that they benefited by using DHS's Procurement Innovation Laboratory (DHS PIL) to improve the efficiency of their cloud acquisition processes.[103] Education officials stated that using DHS PIL resources saved 15 days in the source selection process. Treasury senior officials stated that DHS's PIL aided the agency in tracking contracts, monitoring protest rates, and gathering key acquisition data. SBA officials stated that, following DHS PIL guidance, the agency revised its statement of work to incorporate more granular service descriptions, enabling better price analysis of offers. Several other agencies (e.g., Commerce, DOD, EPA, GSA, and NASA) also established acquisition innovation labs.[104] According to the agencies' websites, the innovation labs were established to support internal acquisition staff in pursuing innovation in agency procurement.

Agencies' Standardized Contract Clauses Designed to Improve Efficiencies

Twelve of the 18 agencies established specific standardized cloud contracting clauses to address existing laws and regulations, and ensure consistency with agency policies on the security of systems and data

[103]DHS established the DHS PIL in March 2015 with the purpose of experimenting with innovative techniques for increasing efficiencies in the procurement process and institutionalizing best practices. Subsequently, in 2021, OMB's OFPP provided the DHS PIL funding, which allowed it to provide federal agencies coaching in federal procurement practices.

[104]"The LAB", Office of Acquisition Management, Department of Commerce, accessed on Jan. 26, 2026. https://www.commerce.gov/oam/lab. "The Acquisition Innovation Research Center", Stevens Institute of Technology, accessed on Jan. 30, 2026. https://acqirc.org/. "Cutting-Edge Contracting Innovation Lab (CECIL)", Environmental Protection Agency, last updated on Mar. 5, 2026. https://www.epa.gov/contracts/cutting-edge-contracting-innovation-lab-cecil. "Procurement Innovation Resource Center (PIRC)" General Services Administration, last updated Feb. 10, 2020. https://www.gsa.gov/policy-regulations/policy/acquisition-policy/procurement-innovation-resource-center. "NASA Acquisition Innovation Launchpad", National Aeronautics and Space Administration, last updated Mar. 5, 2026. https://www.nasa.gov/procurement-nail/.

governance.[105] Specifically, reviews of agency procurement policies, contract guidance, and procurement templates identified standard contract clauses related to data management, security controls, and privacy requirements, among other things. Agency officials reported that the clauses were established with the intention of improving efficiency in the procurement process.

- **Data management clauses.** Eleven agencies developed guidance that included clauses to use in contracts to improve data management for contracts. Education's guidance included regulations that required each contract to include standard clauses that established unrestricted rights to all federally owned or managed data. Similarly, eight agencies developed policies that included standard clauses to be used in contracts that specified the agency's ownership rights to metadata used by contractors. For example, OPM's guidance on IT contract clauses required a specific clause for contracts with cloud providers to allow the agency CIO to access agency information through the contracting officer or contracting officer's representative.[106] The clause allowed OPM to fully and appropriately retrieve its information—including data schemas, metadata, and other associated data artifacts—from the cloud provider.
- **Security clauses.** Five agencies developed guidance on cybersecurity-related clauses for cloud contracts. For example, Education included a clause in all IT contracts requiring contractors to comply with one list of federal and Education information security and privacy requirements.[107] Senior Education officials explained that consolidating the requirements

[105]According to GSA guidance on the Revolutionary FAR Overhaul, agencies are expected to adopt the model deviation text issued by the FAR Council and align agency supplements and policies with the streamlined FAR. Agencies are also expected to engage their acquisition workforce and provide feedback on implementation challenges and successes. Further, agencies are required to provide quarterly updates to OFPP on their adoption of the model deviation text and implementation efforts. See "RFO-Frequently Asked Questions", Revolutionary FAR Overhaul, General Services Administration, accessed on January 30, 2026. https://www.acquisition.gov/far-overhaul/faqs#agency-specific-actions-and-implementation.

[106]Contracting officers are responsible for ensuring a contract meets all requirements of law, executive orders, regulations, and all other applicable procedures, including clearances and approvals, before signature. FAR 1.402-2(a) (deviation). A contracting officer can designate a contracting officer's representative for tasks related to contract execution. FAR 1.404(a)(2) (deviation). The representative must have the proper OMB federal acquisition certification and meet agency-specific requirements.

[107]Education's clause is an example of a clause that was implemented prior to the Revolutionary FAR Overhaul. See Education Acquisition Regulations (EDAR) 3452.239-71 (legacy) Department information security and privacy requirements, which provided for cloud computing security requirements.

into one living document and updating it as federal law, policy, and requirements changed, reduced time contractors spent identifying applicable requirements and made it more efficient for them to meet current federal requirements. In addition, NSF's guidance included clauses that, when included in contracts, would require providers to allow agency officials access to carry out monitoring of contractor facilities, records, and databases, among other things. DHS's guidance featured contract clauses that would make providers fully responsible and accountable for meeting federal security requirements when hosting the agency's systems in a non-DHS data center.

- **Privacy clauses.** Three agencies developed specific standard contract language about privacy in their guidance.[108] For example, Transportation's policy required all cloud contracts to include a clause that would require compliance with a list of specific privacy requirements. DHS's guidance required privacy language in all contracts, including a requirement to establish privacy roles, responsibilities, and access requirements for contractors and service providers.

Training Staff Enhanced Cloud Procurement Expertise

Officials from ten of the 24 agencies reported that the agency provided a variety of training opportunities with the goal of enhancing the staff's expertise in cloud acquisitions. This included:

- **Utilizing external training programs.** Officials from five agencies reported that the agency leveraged external programs like the Digital IT Acquisition Professional program[109] to help staff acquire further expertise

[108]FAR Part 24 (deviation) explains how the *Privacy Act of 1974*, 5 U.S.C. § 552a and OMB Circular No. A-130 (July 28, 2016), apply to government contracts.

[109]The Digital IT Acquisition Professional program is an optional specialized 6-month training program that teaches federal government acquisition professionals to design innovative and flexible procurements for IT and Digital Services. Acquisition professionals gain experience in digital service market intelligence and stakeholder analysis, awarding and administering digital service contracts, and the application of skills learned by shadowing real-world experts in digital service or development. The certification was developed by the United States Digital Service and the Office of Federal Procurement Policy in 2018. "Digital IT Acquisition Professional Training Program (DITAP)", TechFAR Hub, U.S. Digital Service, accessed on January 30, 2026. https://techfarhub.usds.gov/get-started/ditap/.

in IT acquisitions.[110] For example, officials at NRC stated that the certification was beneficial for participants because they shadowed staff at private companies, practiced scenarios, and interviewed stakeholders. In addition, Transportation officials reported that program graduates from various agencies also shared ideas with each other. The officials noted that Transportation had created a fixed unit price model for cloud services, which they shared with other cloud specialists in the broader federal community of certified digital acquisition professionals. Agency officials who mentioned the digital professional certification noted, however, that although the program included some useful information on cloud procurements, it was not specifically tailored for this type of procurement.

- **Participating in communities of practice.** Officials from three agencies reported that participating in government-wide and internal communities of practice helped agency acquisition staff further their knowledge through sharing lessons learned and key practices. Specifically, Justice officials stated that participation in the Cloud and Infrastructure Community of Practice allowed their staff to learn what other agencies had done with cloud contracts, and share lessons learned.[111] Agriculture officials reported that they utilized cloud vendor-specific services and agency communities of practice to connect shareholders whose work focused on operations and acquisition.
- **Developing internal training.** Officials from two agencies reported that the agency had provided internal training opportunities to staff on cloud acquisitions. For example, officials at GSA reported that the agency had developed a credential program for purchasing IT services, which included training on cloud services. GSA officials reported that the

[110]Executive branch general contracting professionals are required to have the Federal Acquisition Certification in Contracting. To receive this certification, a contracting professional is required to have a minimum of twelve months of full-time contracting experience, and must complete a set of core training courses, and pass a professional certification exam. To maintain this certification, contracting professionals are required to take 100 hours of continuous learning every two years. OFPP updated the federal acquisition certification in contracting program requirements in January 2023. See Office of Management and Budget, *Federal Acquisition Certification in Contracting (FAC-C) Modernization* (Washington, D.C.: Jan.19, 2023).

[111]The Cloud and Infrastructure Community of Practice is operated by the GSA IT Modernization Division. The community of practice is designed for federal IT practitioners who want to network with other agencies to learn about common cloud, infrastructure and IT challenges and best practices. After a pause in operations instituted in February 2025, GSA restarted the Cloud and Infrastructure Community of Practice in April 2025.

agency had focused the program on IT as it represented a major category for contract purchases.

OMB and GSA Taking Action to Implement Executive Order on Government-wide IT Procurement Consolidation

OMB and GSA have begun taking action to implement the President's Executive Order to consolidate federal procurement, including IT, issued in March 2025.

On March 20, 2025, the President signed an executive order to consolidate federal agencies' procurement of common goods and services under GSA.[112] The order required the Director of OMB to designate the Administrator of General Services as the executive agent for all government-wide IT acquisition contracts, including cloud contracts, within 30 days of the order. In addition, agency heads, in consultation with the agency's senior procurement officials, were required to submit a proposal to the Administrator of General Services to have GSA procure common goods and services, which included IT, for the agency within 60 days of the order.[113] The order also required GSA to submit a comprehensive plan to OMB for procuring common goods and services, including IT, for the federal government.

In April 2025, GSA began taking action to consolidate federal IT procurement by designating its Administrator with responsibility for all GWACs and for, among other things, identifying and eliminating duplication, redundancy, and inefficiencies in government-wide IT contracts, including cloud contracts.

In addition, GSA launched its OneGov Strategy aimed at modernizing how the federal government purchases goods and services. The strategy is intended to be a comprehensive plan to transform government procurement. Instead of hundreds of separate agency contracts, GSA plans to leverage the collective purchasing power of the entire federal government to secure unprecedented discounts while ensuring consistent

[112]Exec. Order No. 14240, *Eliminating Waste and Saving Taxpayer Dollars by Consolidating Procurement*, 90 Fed. Reg. 13671 (Mar. 20, 2025).

[113]Common goods and services means the common government-wide categories defined by the Category Management Leadership Council. The ten government-wide categories include facilities and construction; human capital; industrial products and services; information technology; medical; office management; professional services; security and protection; transportation and logistics services; and travel.

security standards and simplified access.[114] The agency indicated that it would focus on enterprise software initially because the government had moved from buying software every few years to subscribing to dynamic, cloud-delivered tools. According to the OneGov IT website, as of January 2026, the agency had negotiated agreements for discounts with 19 companies that provide software and cloud services to the federal government.[115]

In October 2025, the FAR Council established the FAR Companion Version 2.0[116] as a result of Executive Order 14275[117] and OMB Memorandum M-25-26.[118] The purpose of the FAR Companion Version 2.0 is to share best practices that empower acquisition professionals to maximize the flexibilities of the FAR, apply sound judgment, balance risk, and effectively and efficiently deliver their agency's mission.

OMB and GSA Have Not Fully Addressed Agency-Identified Cloud Procurement Challenges

Senior officials from the 24 agencies reported that the agencies had experienced several cloud procurement challenges.[119] Specifically, of the 24 agencies,

- 17 reported that tracking cloud costs remains an ongoing challenge for agencies that requires changes in IT cost management;
- 17 reported that OMB-issued SBOM guidance conflicted with NIST guidance and hindered agency implementation of SBOM requirements, including for cloud-related software;

[114]We recently reported that OMB and GSA's current efforts to provide agencies with the tools, training, and expertise needed has the potential to advance category management by driving more spending through government-wide contracts. In doing so, it may also ensure agencies meet their statutory small business contracting goals, address data limitations, and better define requirements. See GAO, *Government Contracting: Leveraging Federal Buying Power Can Save Billions*, GAO-25-108638 (Washington, D.C.: Sept. 29, 2025).

[115]"OneGov IT", General Services Administration, https://itvmo.gsa.gov/onegov/.

[116]Federal Acquisition Regulatory Council, *FAR Companion (FC), Version 2.0* (October 30, 2025).

[117]Exec. Order No. 14275, *Restoring Common Sense to Federal Procurement.*

[118]Office of Management and Budget, *Overhauling the Federal Acquisition Regulation*, M-25-26 (Washington, D.C.: May 2, 2025).

[119]We developed the list of six challenges by reviewing interview responses, agency-provided cloud policies, guidance, and other documentation on challenges such as presentations and lessons learned; federal leading guidance; and prior related reports. All the 24 agencies identified at least one or more of these challenges.

- 15 reported that outdated IT areas and omissions in the FAR have impeded efforts to procure cloud services;
- 15 reported that procuring FedRAMP-authorized cloud solutions is difficult;
- 11 reported difficulties with pursuing multi-vendor cloud procurements due to a variety of constraints; and
- 10 reported that resource constraints hampered acquisition of necessary resources to meet cloud procurement workforce needs.

OMB, GSA, CISA, and other entities have taken various actions to address these challenges. However, not all challenges have been fully addressed.

Agency Cloud Cost Management Remains an Ongoing Agency Challenge

Senior agency officials from 17 agencies reported challenges with managing and reporting costs associated with cloud services. OMB's Circular A-11 states that a disciplined, integrated budget process should provide agency management with accurate information on acquisition and life-cycle costs.[120] In addition, OMB A-130 states that agencies should ensure their data and information needs are met through data governance policies and processes by which agency personnel manage information as an asset.[121]

However, the 17 agencies reported challenges with, among other things:

- **Tracking cloud costs following migration from on-premise environments.** Commerce officials reported that cloud usage and requirements (data volume, bandwidth, throughput, etc.) did not immediately translate one for one with the previously on-premise solution. This created a large degree of uncertainty in the first few years following the migration to cloud services, particularly if the system was mission-critical and could not be turned off. Officials said that the agency might not have the funds to cover unexpected cost overages.
- **Managing costs across different cloud environments.** Interior officials stated that each CSP's cost data was different for the services and tools.

[120]Office of Management and Budget, *Preparation, Submission, and Execution of the Budget*, Circular No. A-11 (July 2024).

[121]Office of Management and Budget, *Managing Information as a Strategic Resource*, Circular No. A-130 (July 28, 2016).

Energy officials reported that ingress and egress costs of moving data into and out of the cloud were problematic.[122]

- **Managing costs in the cloud environment for optimization.** NASA officials explained that continual monitoring, review, and adjustment were needed to reduce costs and optimize the benefits received when using certain cloud models, particularly IaaS. NRC officials stated that understanding the cost implications when making decisions on using reserved instances, evaluating the costs of PaaS versus IaaS, and selecting certain cloud services or contract line-item numbers, had been challenging as the agency had transitioned from a traditional data center to the cloud.[123]
- **Using cloud services requires a fundamental shift in agency IT cost management.** Agency officials reported that their agencies needed to make a fundamental shift from managing cloud costs as capital expenditures to managing them as operational expenditures. For example, senior DOD officials reported that the agency had to transition its approach, contracts, workforce and management to an operational expenditures model to be more effective in the cloud. Labor officials noted that shifting from a capital to operational expenditure model enabled the agency to provision on-demand resources only as needed. Previously, relying on a capital expenditure model had forced large expenditure spending. The shift had provided the agency with better budget control.

OMB's Cloud Smart Strategy notes that agencies need to consider how to maximize value in cloud investments. One way to optimize an agency's cloud environment and spending is through Financial Operations (FinOps). FinOps is an operational framework that combines finance and IT operations to enable organizations to manage and optimize their cloud spending through better financial accountability and collaboration across

[122]Data user fees (ingress and egress) are related to how users transfer and access data in a cloud environment. Data ingress is the process of transferring data into a cloud environment. Data egress occurs when users transfer and access data from a storage location to enable data to be used or processed in some way. While data ingress is often free to users, CSPs generally charge data egress fees for transferring data out of storage, including transferring data from one provider to another, such as at the end of a contract.

[123]Reserved instances provide a way for an agency to get a discount on cloud services by committing to use an instance at a particular price over a specific period. They require specifying an instance type and size as well as a region. GSA's guidance on *FinOps Operational Best Practices* noted that reserved instances are complex to manage and maintain in large cloud deployments. They provide a benefit when there is a known and steady demand for a particular resource type and size for an extended period.

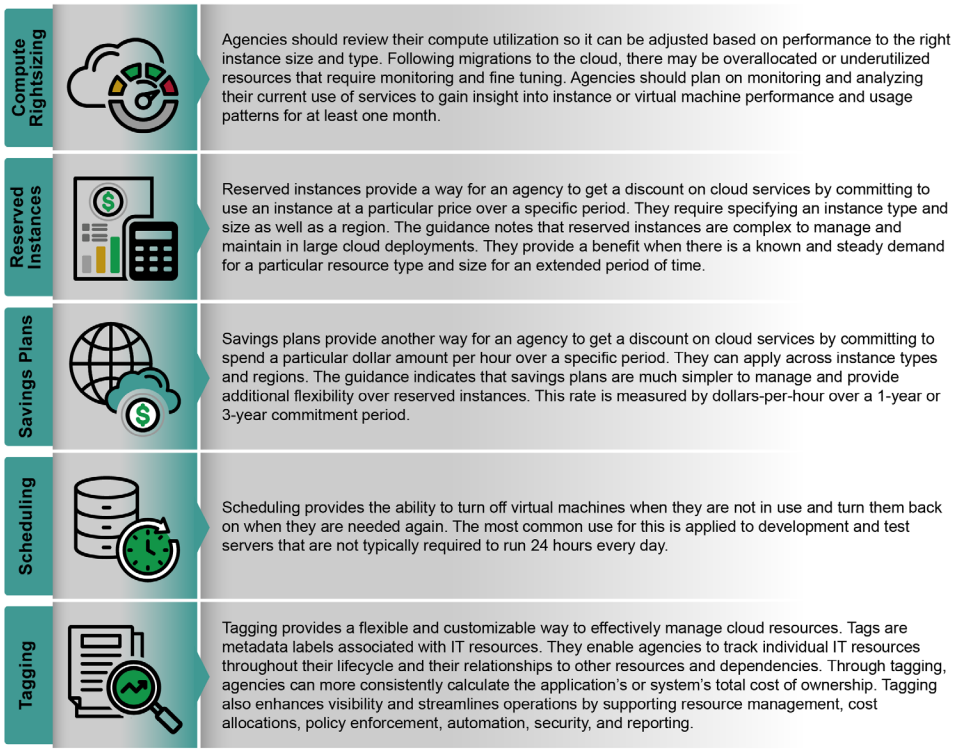
teams.[124] GSA's Office of Government-wide Policy published FinOps operational best practices in 2023 that included high-priority best practices for establishing FinOps metrics.[125] These practices were focused on IaaS services. The guidance also notes that agencies should consider establishing metrics and monthly reporting that is integrated with the overall IT financial management program.

Figure 6 identifies FinOps practices that can be used by federal agencies to optimize cloud environments and achieve cost savings.

[124]FinOps encourages teams to actively monitor and adjust cloud usage according to budget limits and performance goals, as a means of improving cost efficiency and resource allocation. This approach helps organizations balance innovation with cost management, ensuring that cloud investments are both efficient and aligned with organizational objectives.

[125]General Services Administration Office of Government-wide Policy, *FinOps Operational Best Practices* (Washington, D.C.: Jan. 2023). This includes, among others, compute rightsizing, reserved instances, savings plans, scheduling, and tagging.

Figure 6: FinOps Practices That Can Be Used by Federal Agencies to Optimize Cloud Environments and Achieve Cost Savings



Sources: GAO analysis of the General Services Administration's FinOps Operational Best Practices Guidance; Uniconlabs/stock.adobe.com (savings icon); 32 pixels/stock.adobe.com (all other icons). | GAO-26-107530

GSA's Office of Government-wide Policy established FinOps pilots between 2023 and 2024 with seven federal agencies: DOD (Army), Energy, DHS (U.S. Coast Guard), HHS (National Institutes of Health), NRC, OPM, and VA.[126] GSA intended to leverage the findings from the various pilots to document lessons learned, create templates, make recommendations, and provide assessments and analysis as appropriate that could be distributed to the larger government community.

[126]The Consumer Financial Protection Bureau also participated in the FinOps pilot but was not included within the scope of our review. The pilots evaluated the use of FinOps at the agencies to optimize service and performance. Some of the agencies had begun using FinOps prior to the start of the pilot. Pilot results from the Army, OPM, and the U.S. Coast Guard were compiled into case studies to assist other agencies with FinOps implementation.

The agencies reported that participating in the pilots helped them to improve their management of cloud costs and services, as well as achieve some cost savings.

- Senior DOD officials reported that the Army had piloted FinOps and it enabled the agency to begin optimizing its cloud services. For example, the agency collected operational expenditure data in real time so that it could react quickly to reduce spending. The officials said that the agency could see virtual machines that were idle and turn them off to save money.[127] In addition, the agency identified where reserved instances could be used to push data into cheaper storage. One Army division used FinOps and officials reported that they avoided $15.3 million in cloud costs and achieved $11.3 million in cost savings.
- NRC officials reported that the pilot identified several areas where NRC effectively managed its cloud costs and provided a roadmap to fully implement a FinOps program. The officials indicated that the agency had implemented several cost savings measures including reserved instances, power schedules, and managed instances. These measures, the officials reported, resulted in approximately 40 percent in annual savings.
- OPM's FinOps case study stated that the pilot helped the agency establish a policy for tagging cloud costs and reporting to management to provide more visibility into monitoring the agency's cloud costs.[128] The agency integrated FinOps with its existing IT, finance, and procurement functions and obtained discounts from its CSPs for storage. OPM officials reported that the agency achieved more than $500,000 in annual cost savings by adjusting its storage policy and commitments in fiscal year 2023.

GSA officials in the Office of Government-wide Policy stated that the FinOps pilots had demonstrated that agencies could optimize their environments to potentially improve service interoperability and cloud architecture, assist with training staff, and increase security. The officials

[127]Scheduling provides the ability to turn off virtual machines when they are not in use and turn them back on when they are needed again. The most common use for this is applied to development and test servers that are not typically required to run 24 hours every day.

[128]Tagging provides a flexible and customizable way to effectively manage cloud resources. Tags are metadata labels associated with IT resources. They enable agencies to track individual IT resources throughout their lifecycle and their relationships to other resources and dependencies. Through tagging, agencies can more consistently calculate total cost of ownership for the application or system. Tagging also enhances visibility and streamlines operations by supporting resource management, cost allocations, policy enforcement, automation, security, and reporting.

stated that GSA had also leveraged the results of the pilots to identify additional cloud savings opportunities for agencies government-wide. Specifically, GSA officials in the Office of Government-wide Policy stated that the pilots had identified systemic barriers preventing federal agencies from leveraging standard commercial cloud cost-saving mechanisms. These mechanisms included long-term pricing models such as reserved instances and savings plans offered by CSPs—strategies used in FinOps. The officials noted that the barriers included complex procurement requirements (as noted later in our discussion of the FAR challenges).

GSA officials from the Office of Government-wide Policy stated that, based on a cloud forecast analysis that the office had conducted which reflected the projected growth of IaaS across the federal government, agencies will spend approximately $7 billion on IaaS services between 2023 to 2028. The officials said that, assuming a broader government adoption of FinOps principles and optimized use of savings plans, federal agencies could potentially achieve more than $2.35 billion in cumulative savings over that 5-year period, with over $700 million in annual savings by year five alone.[129]

More recently, Executive Order 14240, issued in March 2025, consolidated domestic federal procurement under GSA with the intended goal of eliminating waste and duplication.[130] Under the order, the Administrator of General Services was designated as the executive agent in charge of all government-wide IT acquisition contracts. Further, under OMB M-25-31, the agency was given responsibility for the further reduction of redundant or otherwise inefficient procurement activity within IT contracts, including cloud contracts.[131]

GSA has been working to engage CSPs and interagency partners to explore federal-specific discount structures. As noted previously, according to the OneGov IT website, the agency had negotiated agreements for discounts with 19 companies by January 2026 that provide software and cloud services to the federal government. However,

[129]GSA's cloud forecast analysis projections were based on IaaS spending trends in fiscal year 2023. The analysis also assumed that approximately 55 percent of federal cloud spending was eligible for discount pricing under existing CSP programs.

[130]Executive Order 14240, *Eliminating Waste and Saving Taxpayer Dollars by Consolidating Procurement.*

[131]Office of Management and Budget, *Consolidating Federal Procurement Activities*, M-25-31 (Washington, D.C.: July 18, 2025).

the officials noted that many agencies remain unable to fully leverage the pricing advantages associated with CSP savings plans.

GSA's work on the FinOps pilots has enabled the promotion of a cloud financial operations framework that has many potential benefits for agency cloud procurements. It is also working to address the challenge that exists for the public sector in terms of access to cost-effective cloud pricing. However, enabling agencies to leverage savings plans and reserved instances requires not just internal process improvements, but also systemic reform to federal acquisition regulations, as we discuss later in this report.

GSA officials in the Office of Government-wide Policy agreed that a broader implementation of FinOps across the government could be beneficial to federal agencies. OFPP staff also concurred with the suggestion that agencies implement FinOps. However, OFPP staff did not identify any plans for OMB to provide additional guidance to agencies or require them to implement FinOps.

GSA, as the administrator of government-wide IT contracts, is best positioned to expand the use of FinOps practices across the federal government. By implementing these practices, agencies will be more likely to achieve substantial potential savings. Further, by requiring reporting on the extent of benefits accrued from the use of these practices, GSA will be better positioned to measure the resulting benefits.

Conflicting Guidance Hindered Agency Cloud Software Compliance; Additional CISA Guidance Needed

Officials from 17 of 24 agencies stated that OMB's guidance conflicted with NIST guidance and created challenges for agencies and cloud vendors in meeting two key SBOM requirements—data collection and storage. Agencies rely on SBOMs when acquiring software, including cloud-related software, and use them to manage vulnerabilities and licenses for software already acquired. Accordingly, the President issued Executive Order 14028 in May 2021 and required: (1) NIST to issue guidance that included requirements for vendors to provide an SBOM with each product, including cloud-related products; and (2) OMB to issue guidance requiring agencies to comply with the issued NIST guidance for any software procured after May 2021.[132]

[132]Exec. Order No. 14028, *Improving the Nation's Cybersecurity*, 86 Fed. Reg. 26633 (May 17, 2021).

However, OMB's guidance on SBOM data collection[133] conflicted with NIST guidance[134] and created inefficiencies for agencies. Specifically,

- OMB's M-22-18 guidance indicated that SBOM data collection was optional while NIST guidance noted that software producers should track and share data on all software components for each release using SBOMs with agencies.[135]
- OMB guidance tasked agencies with developing processes for collecting SBOM information from their software producers, including government-wide software producers.[136] NIST's guidance directed software producers to provide SBOM data using standards-based data formats.[137]
- OMB's guidance treated SBOMs as static artifacts for collection and not as data that could be used as a source for vulnerability scanning and risk management as NIST guidance did.[138]

Further, OMB's decision to consider SBOMs as optional compliance artifacts for ensuring secure software development practices created

[133]OMB M-22-18 stated that a SBOM may be required by the agency in solicitation materials based on the criticality of the software or as determined by the agency. Office of Management and Budget, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices.*

[134]NIST addressed the Executive Order 14028's requirement on vendors providing SBOMs to agencies by referencing guidance in the *Secure Software Development Framework Version 1.1*. that noted agencies should track and share SBOM data for each software release. National Institute of Standards and Technology, *Software Supply Chain Security Guidance Under Executive Order (EO) 14028 Section 4e* (Feb. 4, 2022); and *Secure Software Development Framework*, Version 1.1 (2022).

[135]The provenance data on all software components for each release typically includes data such as software producer, component name, component version, software identifiers, dependency relationship, component hash, generation context, license, tool name, timestamp, and SBOM author.

[136]OMB M-22-18 encouraged agencies to notify potential vendors of SBOM requirements as early in the acquisition process as feasible, including leveraging pre-solicitation activities. The guidance also noted agencies should identify whether the software producer was required to provide evidence that it participated in a vulnerability disclosure program.

[137]There are currently two data formats being widely used to generate and consume SBOMs, including Software Package Data eXchange and CycloneDX. These data formats are a product of open, international processes and are both machine-processable and human-readable.

[138]OMB M-22-18 stated that, if an agency required them, the SBOM should be retained by the agency. In addition, agencies should consider reciprocity of SBOMs and other artifacts that were maintained by other federal agencies based on direct applicability and currency of the artifacts.

substantial work and inefficiencies for both agencies and vendors. For example:

- Seven agencies stated that it was inefficient and costly for them to maintain their own SBOM repositories. Specifically, VA senior officials stated that it would be nearly impossible for vendors to maintain comprehensive SBOMs for an agency's products when attempting to comply with each agency's defined standard.
- Five agencies stated that developing a variety of forms and processes among different agencies would create difficulties for providers who work with multiple agencies. For example, officials stated that agencies could have different requirements for the bills of materials, such as the data fields that should be included and the acceptable data formats. The officials noted that government-wide cloud providers would need to replicate the SBOMs for the multiple agencies.
- Five agencies reported that it would be a challenge to collect SBOM information from software providers. For example, agency officials that procured cloud services from a reseller stated that they would be challenged because they did not have a direct relationship with the provider. Therefore, it would be difficult for agencies to collect the SBOMs directly from the providers. Other agency officials reported that software providers have reported that they are unable to provide an SBOM for their software.

In September 2025, CISA released guidance on SBOMs and noted that these data reduced the time to identify and respond to vulnerabilities significantly.[139] This was because the bill of materials was accessible to all participants along the supply chain. Software developers can use the data to develop more secure software and operators can better understand exposure to newly identified risks.

The guidance also noted that:

- an aligned and coordinated approach to bills of materials would improve effectiveness while reducing costs and complexities,
- divergent implementations of SBOMs could hinder widespread adoption and sustainable implementation, and

[139]Cybersecurity and Infrastructure Security Agency, *A Shared Vision of Software Bill of Materials (SBOM) for Cybersecurity* (Sept. 3, 2025).

- SBOM data should be generated, consumed, and analyzed as part of risk management and software development practices, leveraging existing tools where possible.

In addition, according to CISA's guidance, SBOM data can provide agencies with information they can use to make risk-informed security decisions about their software and drive software transparency. Using automated tools, agencies can transform the bill of material data into actionable data that can provide insights on current risks. However, the guidance did not provide specific information on how agencies could integrate SBOM data into agency processes and tools as part of secure development practices.

In January 2026, OMB clarified its guidance on SBOMs.[140] The guidance stated that each agency head was ultimately responsible for assuring the security of software and hardware that was permitted to operate on an agency's network. In addition, the guidance noted that agencies could choose to adopt contractual terms that would require a software producer to provide a current SBOM upon request.[141] OMB's guidance also rescinded previous memorandums in this area, including M-22-18.

While OMB's M-26-05 guidance provided clarification regarding agencies' responsibilities for collecting and maintaining SBOMs, the guidance did not address the other challenges agencies noted. Further, treating SBOMs as optional compliance artifacts will not help to ensure the federal government successfully adopts and implements this key practice.

As mentioned earlier, Congress designated CISA with responsibility for securing information systems and enhancing the security of the nation's critical infrastructure. Therefore, the agency is well-positioned to provide an aligned and coordinated approach to SBOMs. Without CISA issuing additional guidance to federal agencies on how to integrate SBOM data into their risk management and software development practices, agencies will be challenged in adopting this data to make risk-informed decisions.

[140]Office of Management and Budget, *Adopting a Risk-based Approach to Software and Hardware Security*, M-26-05 (Washington, D.C.: Jan. 23, 2026).

[141]OMB M-26-05 stated that agencies that adopted contractual terms for cloud platforms should specify that the producer must provide an SBOM of the runtime production environment upon request.

Outdated IT Areas in the FAR Have Impeded Agency Cloud Procurement Efforts; Efforts Do Not Fully Address Challenges

GSA and OMB have taken action over the past five years to help address four cloud-related challenges with the FAR. In addition, OMB and the FAR Council revised the federal government's regulations as part of Phase One of the Revolutionary FAR Overhaul.

Fifteen agencies reported that outdated IT areas in the FAR have created challenges for them in acquiring cloud services. Specifically, senior agency officials from the Offices of the CIO and Senior Procurement Executive at 15 of the 24 agencies reported that (1) the FAR's (legacy and deviation) definition of commercial product or service did not align with the definition of cloud services, (2) there were challenges with using contract types available in the FAR for consumption-based price models, (3) the FAR (legacy and deviation) had an outdated definition of IT,[142] and (4) the FAR (legacy and deviation) lacked a definition of cloud computing.

The FAR was established for the codification and publication of uniform policies and procedures for acquisition by all executive agencies. It is the primary regulation used by federal agencies to acquire products and services, including acquisitions such as cloud services. The FAR's performance standards as of March 2025 note that the government should maximize the use of commercial products and services. Additionally, the regulatory system must perform in a timely, high quality, and cost-effective manner.

The FAR's definitions of commercial products and commercial services does not align with the parameters of cloud services. The FAR's definitions of commercial products and commercial services,

[142]The FAR includes a section on definitions of words and terms that are frequently used in the regulation or that should be incorporated in solicitations and contracts. FAR 2.101 (deviation).

rooted in statute, have not been updated for decades.[143] Senior agency officials from the Offices of the CIO and Senior Procurement Executive at all 15 agencies reported that the procurement of cloud services was challenging due to limitations with the definitions. For example:

- DHS senior officials reported that classification of cloud services as a service when using the FAR was a challenge because cloud services functioned on a consumption basis, like a utility.[144]
- USAID officials said that the FAR was not flexible in terms of acquiring technology, particularly if the technology was a consumption-based commercial service.
- Interior officials reported that many IT procurements fall within gray areas covered by the FAR. The officials noted that software licensing, not just SaaS, did not fit well within these definitions due to how vendors priced their licenses. Interior officials stated that the vendor market was always evolving and the FAR had not been able to keep up with those changes. Officials noted it has been a challenge to determine which rules to apply to these procurements, particularly cloud procurements.

Senior agency officials from 12 of the 15 agencies stated that the FAR needed to be updated to include a definition related to consumption-based services.

[143]The FAR (legacy) defined a commercial product as a product, other than real property, that is of a type customarily used by the general public or by nongovernmental entities for purposes other than governmental purposes, and has been sold, leased, or licensed to the general public; or has been offered for sale, lease, or license to the general public; a product that evolved from a product described [earlier in] this definition through advances in technology or performance and that is not yet available in the commercial marketplace, but will be available in the commercial marketplace in time to satisfy the delivery. FAR 2.101 (legacy). Commercial services were defined as (1) installation services, maintenance services, repair services, training services, and other services if such services are procured for support of a commercial product as defined in this section, regardless of whether such services are provided by the same source or at the same time as the commercial product; and the source of such services provides similar services contemporaneously to the general public under terms and conditions similar to those offered to the federal government; or (2) services of a type offered and sold competitively in substantial quantities in the commercial marketplace based on established catalog or market prices for specific tasks performed or specific outcomes to be achieved and under standard commercial terms and conditions. FAR 2.101 (legacy). See 41 U.S.C. § 103.

[144]Consumption pricing, consumption basis, or consumption-based model means any offering that is metered with charges that accrue on a predetermined periodic basis (e.g., per second, minute, hour, week, month, or another per-unit basis) and is billed based on actual usage during an elapsed period with predetermined pricing or discounts. This is a pricing structure which allows for invoicing and payment on a use basis.

This is also consistent with the DOD Section 809 Panel's *Report of the Advisory Panel on Streamlining and Codifying Acquisition Regulations*.[145] The report, issued in January 2019, proposed revising the FAR to enable more flexible and effective procurement of consumption-based solutions. Specifically, the report recommended that the products and services model should be updated to provide more flexible purchasing categories that address current and anticipated IT delivery models within the federal government. The report recommended adding a category called consumption-based solutions.[146]

Senior officials from GSA FAS also agreed that the acquisition of cloud services did not fit well into the definition of a product or service as defined in the FAR (legacy). For example, GSA FAS officials explained that one federal agency had considered cloud to be similar to water or electricity, which the FAR would consider a utility. However, the officials noted that the FAR did not describe utilities as a service that would result in a bill that varied by month. In addition, GSA's Cloud Information Center had specifically noted that FAR constraints and the difficulty of treating cloud as a service versus a product had created problems for contracting officers in determining payment options and contract types.[147] GSA has stated that the potential disconnect between treating cloud solutions as either products or services could lead to a host of complications because not all vendor solutions align with the government's buying approach.

[145]Section 809 Panel, *Report of the Advisory Panel on Streamlining and Codifying Acquisition Regulations*, Volume 3 (Washington, D.C.: Jan. 2019).

[146]Section 809 Panel's Report, Volume 3 included a definition for consumption-based solutions as any combination of hardware/equipment, software, and labor/services that together provide a capability that is metered and billed based on actual usage and predetermined pricing per resource unit and includes the ability to rapidly scale capacity up or down. The report had also recommended that traditional services acquisition rules should not apply to consumption-based solutions or to any hybrid contract whose primary purpose was to procure consumption-based solutions.

[147]"Acquisition Challenges" Cloud Information Center, Office of Management and Budget and CIO Council, accessed on July 10, 2025. https://cic.gsa.gov/acquisitions/acquisition-challenges.

Using contract types available in the FAR for consumption-based price models was inefficient and impractical.[148] Senior officials from 10 of the 15 agencies reported difficulties in developing contracts for cloud services due to the FAR's lack of a specific contract type suitable for consumption-based pricing (pay-as-you-go).[149] For example,

- Energy senior officials reported that agencies were required to break out the types of IT that could be procured into different contract types. Energy officials explained that knowing in advance what services were needed, how long the services would be needed, and how to pay for them was a challenge.
- Senior officials from DOD reported that the Air Force had faced challenges contracting for its compute and store cloud services. Officials stated that the Air Force acquired these services through a reseller and a prime integrator under the agency's Cloud One contract using a working capital fund.[150] The officials noted that there were management complexities to using this approach, stating that it required a group of people to manage the number of customers. The officials said that the

[148]The FAR established procedures for the acquisition of commercial products and services (Part 12) and service contracting (Part 37) and when agencies must make payments. The FAR states that a firm-fixed-price is a contract that provides for a price that is not subject to any adjustment on the basis of the contractor's experience in performing the contract. The contracting officer may use a firm-fixed-price contract in conjunction with an award-fee incentive (see 16.402) and performance or delivery incentives (see 16.403 and 16.404) when the award fee or incentive is based solely on factors other than cost. The contract type remains firm-fixed-price when used with these incentives. FAR 16.202-1 (deviation). Fixed price contracts with economic price adjustment provides for upward and downward revision of the stated contract price upon the occurrence of specified contingencies. FAR 16.203-1 (deviation). In addition, the FAR (deviation) provides that a time-and-materials contract may be used only when it is not possible at the time of placing the contract to estimate accurately the extent or duration of the work or to anticipate costs with any reasonable degree of confidence. FAR 16.601-2 (deviation). When included as part of material costs, material handling costs must include only costs clearly excluded from the labor-hour rate. Material handling costs may include all appropriate indirect costs allocated to direct materials in accordance with the contractor's usual accounting procedures consistent with Part 31. FAR 16.601-2(c) (deviation).

[149]In certain circumstances, agencies may pay government contractors in advance for commercial products and services. The contractor is required to provide all resources needed for the performance of the contract. However, in certain instances the contracting officer may include appropriate financing terms in contracts for commercial purchases when doing so will be in the best interest of the government. FAR 32.202-1(a) (deviation).

[150]The Air Force Cloud One contract is managed by a program management office in the Air Force Life Cycle Management Center Cyber and Networks Directorate. The contract is funded using Program Management Office and Mission System Owner funds and is intended to support Air Force cloud applications under one contract. Air Force mission systems were directed to begin moving to Cloud One in June 2021.

work under the contract required more than 400 contract line-item numbers.

To address these difficulties, agency officials reported using the following strategies, contract clauses, and activities to help minimize the impact of the issues identified:

- **Developed additional contract clauses or workarounds.** Five agencies reported developing contract clauses or workarounds. For example, DHS officials reported that one of the components within the department was working to develop a flexible contract line-item number structure that would allow the agency to contract for new services and features more easily. The officials noted that the goal was to require fewer contract modifications and contract supporting documentation, which would reduce the work involved in processing the contracts and speed the migration of services to the cloud. In addition, HHS officials noted that the agency was looking at alternative contract types that would allow them more flexibility to procure cloud services.
- **Sought resources and conducted additional planning.** Three agencies reported that they sought resources and conducted additional planning efforts to address the current challenges. For example, SBA officials reported that the agency had relied on innovative organizations like DHS's PIL to get specific recommendations on handling contracting issues related to consumption-based models. Specifically, SBA officials stated that the agency always included an example list of specific cloud services that would be needed in the statements of work. Implementing this DHS PIL best practice allowed the agency to perform granular, line-item price comparisons across all cloud service offers.

  USAID officials reported that the agency had engaged in extensive planning and administrative activities when it needed to make changes to an existing cloud contract because of the issues related to handling a consumption-based pricing model under a fixed price contract. The officials noted that it had taken time to figure out how to structure the next contract because the agency needed to seek price proposals for the possible consumption levels. The agency also had to determine the size of the environment that was generally needed as well as the parameters of a possible expansion if scaling was necessary.
- **Established a pilot program on consumption-based pricing.** In 2019, DOD's Section 809 Panel issued an acquisitions report that recommended developing definitions, processes, contract types, and funding approaches that aligned with a new category of consumption-

based solutions.[151] Subsequently, in 2021, Congress allowed DOD to establish a pilot program that addressed one of the recommendations in the report. Specifically, through a mandate in the *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021*,[152] the agency developed a pilot program on the use of consumption-based solutions to address software-intensive warfighting capability.[153]

Officials from 12 of the 15 agencies reported that the FAR (legacy) should be updated to better address cloud services and other emerging technologies and the ability to procure these services using a consumption-based pricing model. In addition, eight agencies suggested that a pilot program be conducted on the planned proposed language before the FAR changes were finalized.[154]

This proposed change is also consistent with additional recommendations proposed in the DOD Section 809 Panel's Volume 3 report.[155] Specifically, the report recommended a new contract type to accommodate the uniqueness of consumption-based solutions, noting that it was essential that it be available for commercial acquisitions. The report also recommended that the optimal contract type for consumption-based solutions should function more like a time-and-materials contract

[151]Section 809 Panel, *Report of the Advisory Panel on Streamlining and Codifying Acquisition Regulations*, Volume 3 of 3 (Washington, D.C.: Jan. 2019). This report recommends that the DOD be allowed to use innovative contract types for the procurement of cloud services to be implemented for specific purposes. This includes energy savings performance contracts that allow an energy services contractor to design, finance, acquire, install and maintain energy-savings equipment and systems for a federal agency.

[152]Pub. L. No. 116-283, Div. A, Title VIII, § 834 (Jan. 1, 2021).

[153]A consumption-based solution was defined in the act as any combination of software, hardware or equipment, and labor or services that provided a seamless capability that was metered and billed based on actual usage and predetermined pricing per resource unit and included the ability to rapidly scale capacity up or down.

[154]For example, the General Services Acquisition Manual Part 571 established a pilot program to competitively procure innovative commercial products and commercial services to include innovative technologies and solutions using the commercial solutions opening (CSO) procedure authorized by section 880 of the *National Defense Authorization Act for Fiscal Year 2017* (Pub. L. No. 114-328), as amended by section 7227 of the *National Defense Authorization Act for Fiscal Year 2023* (Pub. L. No. 117-263). The pilot program was designed to be implemented outside the normal FAR requirements to engage traditional and non-traditional government contractors and was intended to promote competition with a streamlined approach to address specific needs for innovative commercial products and commercial services.

[155]Section 809 Panel, *Report of the Advisory Panel on Streamlining and Codifying Acquisition Regulations*, Volume 3 of 3 (Washington, D.C.: Jan. 2019).

rather than a firm-fixed-price contract and automatically capture price reductions in contractors' commercial pricing.[156]

Senior officials from GSA FAS agreed that there had been challenges related to contracting for cloud services. The FAS officials reported that the FAR did not explicitly state that time-and-materials contracts were not allowed for cloud acquisition, so multiple agencies had been using these contracts for this purpose. However, officials from GSA's Office of Information Technology Category said that their technical subject matter experts interpreted the FAR to indicate that time-and-materials contracts could not be used for acquisition of cloud solutions. GSA FAS officials acknowledged, however, that there was a lack of authoritative government-wide guidance on the acquisition of cloud services.

The FAR's definition of IT is not consistent with the definition of IT FITARA. Senior officials from five of the 15 agencies noted that the FAR definition of IT was not consistent with OMB's definition under FITARA. In June 2015, OMB issued an updated definition of IT in accordance with FITARA.[157] The updated definition included references to cloud services and IT support services operated by contractors, reflecting the CIO's additional roles and responsibility. OMB M-15-14 also stated that IT-related definitions should be consistent across IT management and acquisition policies to establish a consistent government-wide interpretation of the definitions. The memorandum stated that the FAR would be updated to be consistent with the IT definition from FITARA.

[156]In December 2025, Congress passed the *National Defense Authorization Act of Fiscal Year 2026.* The Act gave DOD authority to acquire services through consumption-based solutions. In addition, the Secretary of Defense was directed to amend the agency's internal regulation supplement to the FAR to implement the authority granted by Congress to acquire and fund acquisitions for consumption-based solutions. The law defined a consumption-based solution as a model under which a service is provided to the Department of Defense and may utilize any combination of software, hardware or equipment, data, and labor or services that provides a capability that is metered and billed based on actual usage at fixed-price units. See *National Defense Authorization Act for Fiscal Year 2026*, Pub. L. No. 119-60, § 1825 div. A, title XVIII, subtitle C, § 3605(a), 139 Stat. 1248 (Dec. 18, 2025), codified at 10 U.S.C. § 3605.

[157]Under FITARA, the CIO of a covered agency acquired additional responsibility for reviewing the agency's acquisition strategy and plan if it included IT prior to approval. In addition, FITARA stated that the term IT had the meaning given that term under capital planning guidance issued by OMB. As part of M-15-14, OMB established an IT definition under FITARA. Office of Management and Budget, *Management and Oversight of Federal Information Technology*, Memorandum M-15-14 (Washington, D.C.: June 10, 2015).

However, there had been no proposed changes in this regard to amend the FAR in the Federal Register and the FAR had not been updated with OMB's definition of IT under FITARA. The FAR's definition of IT was initially established in 1996 and has remained unchanged since its last revision in 2004.[158] In addition, when compared to the FAR's definition, OMB's definition in M-15-14 contained language related to (1) cloud computing and (2) the lifecycle of the equipment or service, which was missing from the FAR definition (both legacy and deviation).

Agency officials reported that this created additional work for their agencies when they were developing the agency's cloud contracts. Seventeen of 24 agencies' acquisition policies and other contract clause documentation demonstrated that the agencies had taken a variety of approaches to address this issue. For example, both Agriculture's departmental regulation on cloud computing and Justice's procurement guidance document on IT acquisition cited the definition from Clinger-Cohen, but Justice's definition included a reference to specific IT equipment used by personnel in the agency. In addition, USAID's guidance in its automated directive system referred to OMB's M-15-14 and the definition cited there, while OPM's IT contract clause guidance used an agency definition. The officials stated that ensuring more uniformity and consistency with the definition of IT would be helpful.

The FAR does not have a definition of cloud computing. Officials at five agencies reported that this created additional work for their agencies in terms of drafting cloud contracts because the FAR was supposed to reflect terminology that was being used in the current environment. Eleven agency-provided acquisition policies and other contract clause

[158]40 U.S.C. § 11101. The original definition of IT was established under the *Clinger Cohen Act of 1996* and became effective in the FAR in February 1998. Subsequently, minor changes to the definition of IT were passed by Congress under the *Consolidated Appropriations Act of 2004* in January 2004.The changes became effective in the FAR in April 2006. See Federal Register, *Federal Acquisition Regulation; Information Technology Management Reform Act of 1996,* 62 Fed. Reg. 64914 (Dec. 9, 1997) and *Federal Acquisition Regulation; FAR Case 2004-030, Definition of Information Technology*, 75 Fed. Reg. 20298 (Apr. 19, 2006).

documentation referenced NIST's definition of cloud computing in their contract guidance and clauses, and FAR supplements.[159]

OMB staff reported that they had included a definition of cloud computing in a proposed FAR rule on cybersecurity requirements for unclassified federal information systems. The staff said the proposed rule was placed in the Federal Register in October 2023.[160] A review of the proposed FAR rule determined that the definition of cloud computing utilized the definition from NIST SP 800-145. However, as of May 2026, the rule had not yet been finalized. In addition, GSA officials from the Office of Information Technology Category stated in June 2025 that the plan was still to include the NIST definition in the revised FAR Overhaul once it was completed. Phase One of the Revolutionary FAR Overhaul was completed in October 2025, and the deviation to FAR 2.101 did not include a definition for cloud computing.[161]

GSA and OMB Made Federal Regulation Reforms, but Cloud-Related Challenges Remain

GSA and OMB have taken several actions over the past 5 years to address challenges with contracting for cloud solutions that senior agency officials in the Offices of the CIO and Senior Procurement Executive have identified. In particular:

GSA issued acquisition letters to assist agencies with buying cloud services on a consumption basis. Under the FAR, GSA has the authority to establish ordering procedures for contracts on the Federal Supply Schedule. To help facilitate federal procurement, GSA's Senior Procurement Executive issued two acquisition letters related to purchasing cloud services. In particular:

- In December 2021, GSA's Senior Procurement Executive issued Acquisition Letter MV-21-06 to the agency's acquisition workforce.[162] The letter established special ordering procedures for buying commercial

[159]NIST's definition focuses on solutions that exhibit the five essential characteristics of cloud computing: on-demand service, broad network access, resource pooling, rapid elasticity, and measured service. See National Institute of Standards and Technology, *The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology*.

[160]Federal Register, *Federal Acquisition Regulation: Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems*, 88 Fed. Reg. 68402 (Oct. 3, 2023).

[161]FAR 2.101 (deviation).

[162]General Services Administration Office of Governmentwide Policy, *Procurement of Cloud Computing on a Consumption Basis under the Federal Supply Schedule Program*.

cloud services on a consumption basis under the Federal Supply Schedule. The letter also specified that the contract clause would remain in effect until rescinded, or upon incorporation into the FAR.[163] While the letter assisted agencies that used specific GSA cloud contracts, the letter's procedures would not help agencies that utilized non-GSA contracts.

- Subsequently, in March 2024, GSA's Senior Procurement Executive issued Acquisition Letter MV-2024-01.[164] The letter provided guidance to contracting officers who might have questions about purchasing SaaS and how payment for these services could be made. While the memo assisted agencies that established contracts for SaaS cloud services, the letter's guidance would not help agencies that utilized other cloud service models that were not SaaS products.

OMB and the FAR Council's overhaul made changes to acquisition regulations but did not address cloud procurement challenges. OMB and the FAR Council revised all 53 parts of the FAR from April 2025 through October 2025 as part of Phase One of the Revolutionary FAR Overhaul.[165] This included the parts related to definitions (Part 2), products and services (Part 12), and contracts (Part 37) that created cloud procurement challenges for senior agency officials. In addition, the FAR Council developed the FAR Companion Version 2.0 to help acquisition officials exercise their discretion.[166] The companion guidance provides context, additional information, and practical advice for planning,

[163]GSAR 552.238-116 (legacy).

[164]The letter noted that advance payments were a specific type of contract financing method where payments were made prior to delivery of completion of the product or service. In the context of software licenses delivered or accessed via SaaS, payment was often made upfront. The letter clarified that, under specific conditions, an upfront payment was not considered an advance payment. See General Services Administration Office of Governmentwide Policy, *Guidance on Payment for Software Licenses Delivered via SaaS*.

[165]The President's Executive Order called for OMB and the FAR Council to amend the FAR so that it contained only provisions required by statute or that were otherwise necessary for sound procurement. The order also called for consistency and alignment of agency supplemental regulations and internal guidance with the changes made to the FAR. See Exec. Order No. 14275, *Restoring Common Sense to Federal Procurement*, 90 Fed. Reg. 16447 (Apr. 15, 2025).

[166]Federal Acquisition Regulatory Council*, FAR Companion, Version 2.0*.

awarding, managing, and closing out contracts, consistent with the FAR's core buying principles.[167]

As part of the FAR Council's changes to the acquisition regulations, guidance was issued that addressed consumption-based technologies for the first time. Specifically, the *FAR Companion Version 2.0* described firm-fixed-unit-price contracts, which the guidance said could be suitable for consumption-based technologies.[168] The guidance noted that a firm-fixed-unit-price contract might be suitable for procuring cloud computing or other information technology where the supply or service could be described in terms of usage rather than a specific product or task.

While the revised FAR included many significant changes to acquisition regulations, the changes did not address the identified cloud procurement challenges. While the *FAR Companion Version 2.0* included guidance on a firm-fixed-unit-price contract that could be suitable for consumption-based technologies, it is too soon to tell if this will be sufficient to address agency needs. In addition, other challenges related to definitions in the FAR were not addressed. Table 1 below details our evaluation of the Revolutionary FAR Overhaul's changes to the FAR related to the agency-reported cloud procurement challenges.

[167]The FAR Companion guidance includes a disclaimer clarifying that the information in the guide is intended to be used to understand the FAR and related procurement principles. In addition, the disclaimer states that guide does not constitute mandatory compliance requirements. The disclaimer further states that adherence or non-adherence to the advice, instructions, explanations, or interpretations provided within the guide is not intended to carry legal authority nor is it intended to serve as the basis for protests or legal actions.

[168]A firm-fixed-unit-price contract is defined as a contract that establishes a fixed price for supplies or services but does not establish a quantity, except for a guaranteed minimum and ceiling. A firm-fixed-unit-price contract may be structured on a consumption basis, in which a fixed-price is established for a unit of usage, such as a resource unit, and supplies and services are metered and billed based on actual usage over a predetermined periodic basis. A type of FFUP contract is a consumption-based contract. See FC 16.2 in Federal Acquisition Regulatory Council*, FAR Companion, Version 2.0* (October 30, 2025).

Table 1: Assessment of Federal Acquisition Regulation (FAR) Overhaul Revisions That Address the Agency-Reported Cloud Computing Federal Regulation Challenges Reported by 15 Selected Federal Agencies, as of January 2026

Challenge identified	FAR (legacy)[a]	FAR (deviation)[a]	GAO assessment
FAR (legacy) did not include a definition of a commercial product or service that would align with the parameters of cloud services.	The FAR (legacy) definitions of commercial product and commercial service do not account for consumption-based technologies. FAR 2.101 (legacy) These definitions, rooted in statute, were based on the definition of a commercial item, established in 1994 several years prior to cloud services. In 2018, the definition of a commercial item was split into product and service. The two definitions did not change from original definition of an item.	The FAR (deviation) included minor changes to the definitions of commercial product and commercial service in Part 2 from the prior version. FAR 2.101 (deviation)	The changes to the definition of a commercial product and commercial service in the FAR (deviation) appear to focus on making the text clearer and more concise rather than changing the definitions of the terms included in the FAR (legacy). FAR 2.101 (legacy and deviation) While it is beneficial to facilitate ease of understanding and clarity in definitions, the Revolutionary FAR Overhaul did not address the challenge. The definitions for commercial product and service are still thirty years old and remain outdated. Updating the definitions would ensure federal regulation aligns with the current technological landscape.
FAR (legacy) lacked a specific contract vehicle suitable for consumption-based pricing.	The FAR (legacy) allowed for various contract types, including fixed price, time-and-materials, and cost reimbursement. Agency officials reported that none of these specific contract models were suitable for consumption-based or pay-as-you-go pricing. FAR 16.202-1, 16.601 (legacy)	The FAR (deviation) clarified policies and procedures for selecting contract types but did not alter the contract types available. FAR 16.202-1 (deviation) The *FAR Companion Version 2.0* section 16.2, however, contained guidance related to consumption-based cloud contract models. The section noted that agencies could use a firm-fixed-unit-price contract that could be structured on a consumption basis. The section also stated agencies could establish a fixed price for a unit of usage and services could be billed based on actual usage over a predetermined basis. See Federal Acquisition Regulatory Council, *FAR Companion, Version 2.0* (October 30, 2025).	The *FAR Companion Version 2.0* provides some basic guidance on a contract model that can be used for consumption-based technologies, including cloud computing. It is too soon to tell if this guidance will be sufficient to address agency needs.

Challenge identified	FAR (legacy)[a]	FAR (deviation)[a]	GAO assessment
FAR (legacy) definition of IT is not consistent with the definition of information technology in FITARA.	The Office of Management and Budget (OMB) established the federal government's current definition of IT in 2015 in accordance with the Federal Information Technology Acquisition Reform Act (FITARA). This definition included references to cloud services and IT support services operated by contractors, reflecting the Chief Information Officer's additional roles and responsibility under FITARA. The FAR's (legacy) definition of IT—originally established in 1996 and rooted in statute—has not been updated since 2004. FAR 2.101 (legacy)	The FAR (deviation) did not include any changes to the definition of information technology. FAR 2.101 (deviation)	The FAR's (legacy and deviation) current definition of IT was last updated in 2004 and lacks any reference to cloud services. Updating the definition to match the definition currently used by OMB and the federal government, in accordance with FITARA, would provide more consistency in terminology for federal acquisitions.
FAR (legacy) lacked a definition of cloud computing.	The FAR (legacy) does not have a definition of cloud computing. FAR 2.101 (legacy)	Phase One of the Revolutionary FAR Overhaul was completed in October 2025 and did not include a definition for cloud computing. FAR 2.101 (deviation)	The FAR (legacy and deviation) does not have a definition for cloud computing. FAR 2.101 (legacy and deviation) OMB and the federal government rely on the National Institute of Standards and Technology's definition of cloud computing. Adding a cloud computing definition to the FAR (deviation) would provide consistency in terminology for federal acquisitions.

Source: GAO analysis of agency interviews and FAR (legacy and deviation) guidance documentation. | GAO-26-107530

[a]The version of the FAR prior to the Revolutionary FAR Overhaul is called the FAR (legacy). The subsequent version after the overhaul is called the FAR (deviation).

As directed by executive order, the Revolutionary FAR Overhaul is to return the FAR to its statutory roots. It is only to include regulations required by statute or that are otherwise necessary to support simplicity, usability, and strengthen the efficacy of the procurement system. Accordingly, statutory changes are appropriate to address the acquisition challenges agencies have identified.

Congress established the current definitions for commercial products and commercial services (based on the definition of commercial items) in

statute in 1995.[169] However, agencies' challenges with these definitions have created inefficiencies in cloud contracts—a key component for the modernization of federal IT infrastructure. Without congressional intervention to make changes to these statutory definitions, and subsequently the FAR, federal agencies will likely miss key contracting opportunities. Pursuing opportunities in the development and use of technologies such as cloud computing, quantum computing, and artificial intelligence can help transform the federal IT landscape.

Further, Congress's passage of FITARA in 2014 provided federal agencies with an updated IT definition that aligned with CIO responsibilities under the new legislation.[170] However, federal agencies must still rely on the definition last updated in 2004 for FAR contracting actions.[171] In addition, Congress has not yet established a definition for cloud computing in statute that would be required to be included in the FAR. The FAR defines key terms to prevent misinterpretations of technical terms, and to ensure clarity, consistency, and uniformity in the federal acquisition process. Without congressional intervention to update key cloud-related terms in statute, agencies will continue to struggle with ensuring their cloud contracts are consistent with federal definitions and guidance.

[169]The definition of a commercial item was added to the FAR in 1995 after Congress passed *The Federal Acquisition Streamlining Act of 1994.* Federal Register*, Federal Acquisition Regulation; Acquisition of Commercial Items*, 60 Fed. Reg. 48231 (Sept. 18, 1995). The FAR was amended in December 2021 to implement section 836 of the *John S. McCain National Defense Authorization Act for Fiscal Year 2019*, which redefined and required the separation of the definition of commercial items into commercial products and commercial services. The revised definitions were a recommendation of the DOD's Section 809 panel. The panel recommended that Congress split the definition of commercial items into two separate definitions—commercial products and commercial services. The Section 809 panel was created under section 809 of the *National Defense Authorization Act for Fiscal Year 2016* to review and improve the functioning of the defense acquisition system and eliminate any regulations found unnecessary to achieve such improvements. Pub. L. No. 114-92, § 809 (2015).

[170]The law stated that the term "information technology" has the meaning given the term under the capital planning guidance issued by OMB. *Carl Levin and Howard P. 'Buck' McKeon National Defense Authorization Act for Fiscal Year 2015*, Pub. L. No. 113-291, division A, title VIII, subtitle D, § 831, 128 Stat. 3292, 3439 (Dec. 19, 2014). 40 U.S.C. § 11319. OMB established a new definition for IT in M-15-14 in accordance with FITARA. See Office of Management and Budget, *Management and Oversight of Federal Information Technology*.

[171]40 U.S.C. § 11101(6). The law, initially titled *the Information Technology Management Reform Act*, was subsequently renamed the *Clinger-Cohen Act of 1996* in Pub. L. No. 104-208, (Sept. 30, 1996).

Agencies Took Action to Address FedRAMP Authorization Challenges; OMB and GSA are Making Changes

Officials from 15 agencies reported challenges with finding vendors that had received FedRAMP authorization. Specifically, costs and other factors deterred vendors from obtaining FedRAMP authorization. Officials from 11 of the 15 agencies reported that they had not been able to procure cloud services or had to significantly delay the procurement of certain products, because the vendor was not able or willing to go through FedRAMP. For example, Interior officials stated that small companies generally did not have the resources to invest in becoming FedRAMP-authorized. HUD officials reported that the agency started to go through the procurement process with a FedRAMP-certified vendor. However, during the process, the vendor decided to discontinue their authorization because it was too costly to maintain, and the return on investment was not enough to maintain the FedRAMP authorization. As a result, according to the officials, HUD had to find another vendor and start the procurement process over again.

In our recent work on the costs of FedRAMP authorization, we found that estimates of the costs associated with pursuing a FedRAMP authorization varied widely.[172] For example, of the agencies that reported costs, nearly all ranged from $69,000 to $400,000, with a few as low as $12,000 and one as high as $706,000. In addition, two CSPs that were small businesses incurred costs for updating their infrastructure (ranging from $367,000 to $3,000,000). The lack of OMB guidance on reporting authorization costs was a contributing factor to the wide variance in estimates. We therefore made a recommendation to OMB to issue guidance on tracking and reporting FedRAMP sponsorship authorization costs. OMB took action to address our recommendation in July 2024 by issuing M-24-15.[173]

Agencies also faced barriers that impeded their implementation of FedRAMP-authorized solutions. Officials from 11 of the 15 agencies reported cases where they could not procure cloud services due to delays with FedRAMP authorization or because they could not determine which service offering had received the authorization.[174] For example, Transportation officials stated that the agency had tried sponsoring vendors for FedRAMP authorization but had two vendors withdraw in the

[172]GAO-24-106591.

[173]Office of Management and Budget, *Modernizing the Federal Risk and Authorization Management Program (FedRAMP).*

[174]Agencies can use the FedRAMP Marketplace's publicly available database to research and identify secure cloud services that are available for government-wide use.

middle of the process. SBA senior officials reported that the FedRAMP process was too slow in onboarding new technologies and services. SBA officials added that not enough products were granted authorization, given the speed at which new technologies and services were made available each year. Officials also noted that it could be challenging to determine which cloud services were FedRAMP-authorized when major cloud providers had authorization but had services in their catalogs that were not authorized.

Our prior work on FedRAMP authorization costs also noted these issues.[175] Four agencies (DHS, HHS, Treasury, and VA) reported that CSPs were not always fully prepared when initially pursuing authorizations. Officials from the four agencies reported that CSPs did not always fully understand the FedRAMP process and lacked complete documentation.

Agencies have taken a variety of actions to address FedRAMP procurement challenges, including sponsoring cloud vendors, partnering with other agencies, or accepting the risk of using a non-FedRAMP-authorized provider. For example, Justice officials stated that the agency was supportive of the FedRAMP process and encouraged component agencies, particularly with emerging technologies, to look at sponsoring a company through the process. In addition, Education officials stated that the agency had reached out to other agencies to try to partner with them to encourage vendors to become FedRAMP-authorized. Further, NASA senior officials reported that the currently authorized cloud services were not able to meet all of the agency's diverse mission requirements, particularly for collaboration with the scientific community. NASA officials noted that the FedRAMP Marketplace does address many of the major cloud offerings available. However, the cloud services authorized under FedRAMP represent less than 1 percent of the cloud services available commercially.

In July 2024, OMB issued M-24-15 that aimed to modernize FedRAMP.[176] The memo outlined an updated vision, scope, and governance structure designed to be responsive to developments in federal cybersecurity and made substantial changes to the commercial cloud marketplace that had occurred since the program was established. Specifically, M-24-15 made

[175]GAO-24-106591.

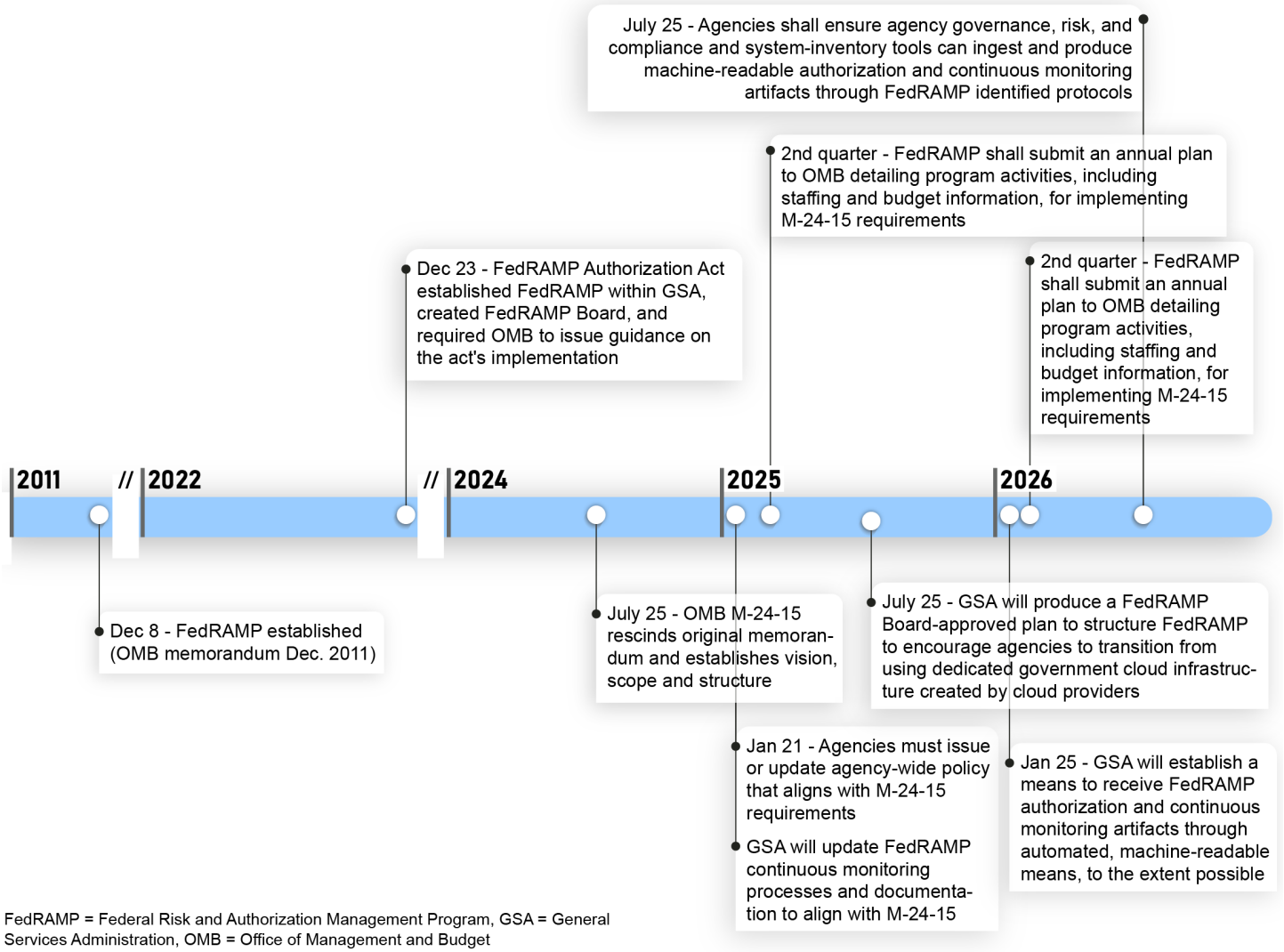
[176]Office of Management and Budget, *Modernizing the Federal Risk and Authorization Management Program (FedRAMP)*.

changes to the FedRAMP authorization paths and streamlined the program's authorization processes. For example, OMB's memo offers additional paths for authorization of cloud services. More specifically, there are FedRAMP-provided procedures for issuing a time-specific temporary authorization to identify more cloud service offerings that could become FedRAMP-authorized, and to accelerate the agency's eventual path to authorization.

In addition, FedRAMP was directed to create guidance that supported CSPs and agencies in streamlining the authorization process for cloud products and services that use FedRAMP-authorized infrastructure or platforms. In addition, the memo directed GSA to establish a means of automating FedRAMP security assessments and reviews and supporting agency CSP reuse of an existing authorization. Further, the memo required agencies to report the costs associated with the issuance of FedRAMP authorizations, in accordance with OMB budget guidance.

If implemented effectively, these changes to FedRAMP could potentially address the authorization challenges reported by agencies when implemented. The timeline in figure 7 outlines the planned implementation of the activities as described in M-24-15.

Figure 7: Required Actions and Deadlines Established in Office of Management and Budget Memorandum M-24-15 Regarding Planned Implementation of Updates to FedRAMP



FedRAMP = Federal Risk and Authorization Management Program, GSA = General Services Administration, OMB = Office of Management and Budget

Source: GAO analysis of federal law and OMB guidance on FedRAMP. | GAO-26-107530

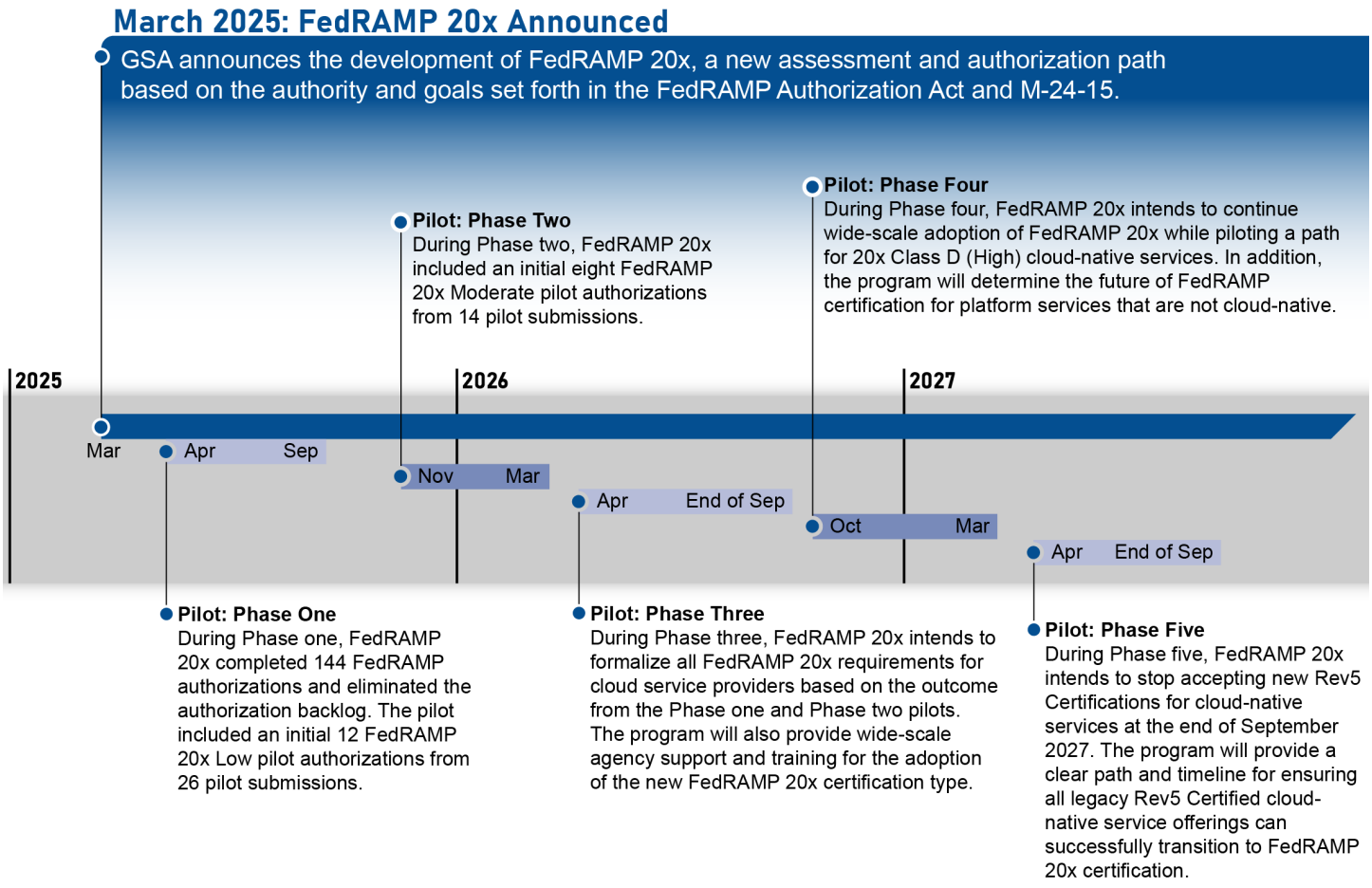
In addition, GSA officials stated that, in March 2025, the FedRAMP office had initiated FedRAMP 20x, an initiative to partner with industry on a new approach for authorization. FedRAMP 20x will focus on building and iteratively improving a new authorization process that is designed to be simple to automate. This will allow companies to continuously and efficiently validate the underlying security of their services. For example,

one of the goals of the initiative will be to have 80 percent or more of the program requirements be able to be validated through automation.

Further, GSA officials noted that they had an effort underway that was intended to improve authorization data. In April 2025, the FedRAMP office began a pilot of a standard for storing and sharing authorization data. The standard defined requirements for CSPs to store and share these data with agencies using their existing commercial processes and trust centers.[177] The timeline in figure 8 outlines the current and planned implementation of phased activities for FedRAMP 20x.

[177]The intent of this standard is to meet the requirements under *The FedRAMP Authorization Act*. The act required the Administrator of General Services to provide a secure mechanism for storing and sharing necessary data, including FedRAMP authorization packages, to enable better reuse of such packages across agencies, including making available any information and data necessary for agencies. This responsibility was delegated to the FedRAMP Director.

Figure 8: Current and Planned Implementation Phased Activities for FedRAMP 20x, as of May 2026



FedRAMP = Federal Risk and Authorization Management Program

Source: GAO analysis of FedRAMP documentation. | GAO-26-107530

As of May 2026, FedRAMP 20x is currently in Phase three and the program is focused on delivering the final activities necessary to establish certification types for use. FedRAMP 20x requirements are expected to be finalized by the end of June 2026. Submissions for the program are planned to open between July through September 2026.

In addition, as noted previously, agencies have used the FedRAMP Marketplace's database to search for cloud service offerings that have achieved a FedRAMP designation. As part of the new authorization data sharing process, CSPs will be required to provide descriptions of their services that have received FedRAMP authorization.

OMB's and GSA's efforts to modernize FedRAMP, including additional paths for authorization and efforts to streamline the processes, are key improvements to the program. In addition, the FedRAMP office's efforts to automate authorization processes has the potential to lower costs, not only for those CSPs interested in becoming authorized, but those seeking to maintain their authorization once it is fully implemented.

Agencies' Multi-Vendor Cloud Procurements Impacted by Insufficient CIO Council Guidance

Multi-vendor cloud procurement is a strategy of pursuing a wide range of CSPs rather than relying on a single provider for all the agency's cloud services. This strategy allows the agency to diversify across multiple cloud platforms and help avoid vendor lock-in.[178] Interoperable cloud technologies allow the different cloud platforms, applications, and services within an agency to communicate and exchange data. However, supporting a multi-cloud strategy or multiple cloud platforms also has technical, security, workforce, and cost considerations.[179]

Congress has designated the CIO Council with the responsibility for sharing experiences, ideas, best practices, and innovative approaches for information resources management.[180] To meet its responsibilities, the CIO Council has a strategic goal of driving agency adoption of cloud services and providing access to cloud best practices.

Senior officials from 11 of 24 agencies reported an ongoing challenge in developing strategies to use multi-vendor cloud solutions and technologies.[181]

[178]Vendor lock-in describes the practice of platforms or technologies that "lock" customers into a particular product, limiting their ability to change vendors in the future.

[179]A multi-cloud architecture refers to the use and integration of cloud services from multiple CSPs. While SaaS and PaaS can be part of a multi-cloud architecture, the term generally refers to IaaS offerings, where the customer is responsible for configuring the underlying compute, storage, network, and other foundational resources.

[180]E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2905-06 (Dec. 17, 2002) (44 U.S.C. § 3603).

[181]Examples of technologies designed to run in a multi-cloud environment include containerization, orchestration, infrastructure as code, and continuous integration/continuous delivery pipeline. Containerization allows software to be bundled together independent from the underlying hardware and operating system. Orchestration automates the deployment and management of the containers. Infrastructure as code manages and provisions computing infrastructure through machine-readable configuration files rather than manual setup. Continuous integration/continuous delivery pipelines allow organization to quickly build and test code changes to maintain a consistent code base for applications while dynamically integrating code changes.

- **Multi-vendor cloud solutions require significant management, staffing, and financial resources for implementation.** DOD officials reported that a multi-vendor solution required more expertise, time, tooling, and resources because it required open standards, open application programming interfaces, cloud native computing applications, and containers. Further, OPM officials reported that containers required quite a bit of maintenance and patching and the availability of staff with skills in multiple cloud platforms was limited. Transportation and USAID officials stated that it was a challenge to develop effective and timely strategies to use these solutions. Energy officials noted that specific uses of these container orchestration tools would be challenging to implement and to also obtain the proper accreditation.

- **Choosing technologies and architectures that will run seamlessly across multiple cloud providers requires numerous technical considerations.** Labor officials explained that it was a challenge to find solutions that were truly vendor neutral. The officials said that typically there were portions of the service, such as containers, code, and general practices, that did not rely on a single cloud vendor's proprietary technology. However, the underlying technologies, best practices, cost models, governance, security, and service restrictions generally did rely on proprietary technology.

GSA has established several areas of multi-vendor cloud procurement guidance to help agencies in their implementation efforts. This included establishing a multi-cloud or hybrid strategy,[182] assessing readiness for containerization technology,[183] and documenting FedRAMP container vulnerability scanning resources.[184] The CIO Council developed, in coordination with GSA, a guide on cloud operations best practices and resources that includes a brief overview of multi-cloud and hybrid cloud environments, the advantages and disadvantages, and a link to GSA's guidance in this area.[185] The website also maintains links to FedRAMP

[182]General Services Administration Office of Government-wide Policy, *Multi-Cloud and Hybrid Cloud Guide*.

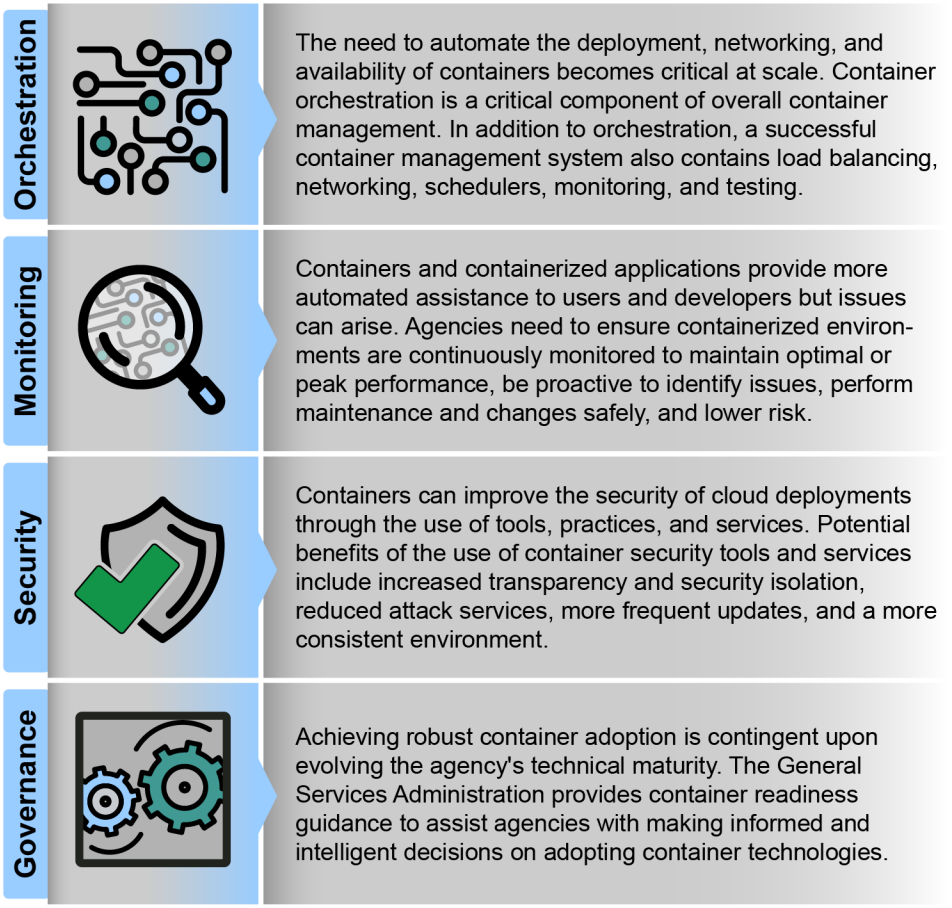
[183]General Services Administration Office of Government-wide Policy, *Containerization Readiness Guide* (May 12, 2021).

[184]General Services Administration, *FedRAMP Vulnerability Scanning Requirements for Containers* (March 16, 2021).

[185]General Services Administration and CIO Council, *Cloud Operations Best Practices and Resources Guide* (Oct. 2023).

and other materials.[186] Figure 9 below outlines four key areas that agencies need to consider when managing containerization technology.

Figure 9: Four Areas Agencies Need to Consider for Containerization Management According to Federal Guidance



Sources: GAO analysis of federal container guidance; 32 pixels/stock.adobe.com (all icons). | GAO-26-107530

Four agencies reported that they were using containerization and other technical approaches as part of their agency's overall multi-vendor cloud strategy. Specifically,

[186]The CIO Council's website listed a presentation related to secure cloud computing that included a slide on the benefits of the hybrid cloud model. See Scott Renda, "One Cloud Does Not Fit All: Adopting a Secure Cloud For Government", PowerPoint Presentation, Office of E-Government and Information Technology, Office of Management and Budget, May 13, 2014.

- VA officials reported that the agency had created Platform One, a container orchestration platform that supported automation and more rapid development of functionality. The platform was launched in 2021. The agency had wanted to standardize its cloud services and create an enterprise approach to maximize efficiency. The platform has gradually gained adoption throughout the agency as contracts have been switched over and new projects have begun. Platform One runs on top of the VA Enterprise Cloud and the on-premise data centers, which has helped to speed the migration of applications from an on-premise environment to the cloud.
- DOD officials reported that a multi-cloud environment was the only appropriate solution for the agency because of its size and mission-critical needs. In addition, the agency focused on a technical architecture that adopted open standards. This included the use of containers, microservices,[187] and sidecar security containers,[188] which helped to enhance cloud cybersecurity.
- GSA officials reported that the agency supported multiple container platforms that run its business systems and web applications. The officials indicated that this included both vendor and cloud-native platforms.
- SSA officials reported that the agency used a hybrid cloud application platform that assisted in the development, deployment, and management of containerized applications.

However, officials from seven agencies reported that more guidance was needed to help address the policy and technical challenges of using containerization and multiple cloud services as part of a multi-vendor cloud strategy. For example, officials from Justice and NRC suggested that there needed to be additional testing to ensure that major cloud

[187]Microservices, and using a microservice architecture, is an approach to application development in which a large application is built as a collection of modular, loosely coupled components or services. Each microservice typically runs inside a software container. See National Institute of Standards and Technology, *Security Strategies for Microservices-based Application Systems*, Special Publication 800-204 (Aug. 2019).

[188]Sidecar security containers help to build security into the application without requiring any action from the application development team. Container orchestration packages a group of containers into pods. Each pod may contain several containers, and containers within pods can share disk and network resources. A sidecar container is a container used to extend or enhance the functionality of an application container without strong coupling between the two. The use of pods makes it possible to create a sidecar security container and automatically deploy an instance of it in each pod alongside each application container, building security into the application. See Department of Defense, *Cloud Security Playbook Volume 2* (Washington, D.C.: Feb. 11, 2025).

service platforms were interoperable. Justice officials noted that this was important, as federal agencies would all be faced with this challenge if they procured services from multiple providers. The officials said it would ensure a unified government approach with the vendors.

GSA officials from the Office of the CIO recommended developing repeatable macro and micro pattern standards for use-case specific containerization architectures and integration capabilities. This would help facilitate additional standardization of containerization across the government, particularly around the configuration of components and services, version control, and code development. Further, Commerce officials recommended that OFPP issue a government-wide mandate that required agency cloud acquisitions to have the capability to be interoperable.

Although it has the responsibility for sharing governmentwide leading practices, the CIO Council provided minimal cloud guidance, focusing on one FedRAMP priority. Without the CIO Council facilitating the collection and sharing of information on federal government leading practices on multi-vendor cloud solutions, including containerization and platform interoperability, agencies will likely continue to struggle to successfully implement these solutions.

Agency Resource Constraints Hampered Cloud Procurement Workforce; GSA and CIO Council Are Developing Guidance

Senior officials from 10 of the 24 agencies reported challenges with hiring and retaining skilled staff for the procurement of cloud services. OMB's Cloud Smart Strategy notes that agencies need to recruit and hire staff to address skills gaps in the cloud workforce.[189] These strategies should include leveraging industry recruitment best practices, expanding the use of pay flexibilities, and removing bureaucratic barriers to hiring staff expeditiously. In addition, one of the CIO Council's strategic goals is to provide the federal government with a workforce of highly capable IT professionals with mission-critical competencies to meet agency goals.

However, agency officials reported that their agencies experienced challenges with (1) finding skilled staff with the necessary expertise in cloud services and cloud procurement, and (2) competing with the private sector's salary and benefits. For example, VA officials stated that the agency was focused on finding staff with the necessary breadth and depth of cloud expertise.

[189]Office of Management and Budget, *Federal Cloud Computing Strategy.*

Energy and HHS officials reported difficulty competing with the private sector for skilled workers due to pay differences and more streamlined hiring processes that allowed new hires to acquire skillsets immediately. Agriculture officials also noted that they had lost skilled staff to the private sector and had needed to rely on contractors to fill certain positions. SSA officials noted that the shortage of staff, including for cloud procurement, would continue to be an issue as contracting officers retired or left the agency.[190]

To help address these challenges, agencies developed internal workforce programs.

- State officials reported that they created the agency IT Skills Incentive Program to provide retention benefits for agency IT staff. Participating staff would receive base salary increases for earning industry certifications or acquiring bachelor's or master's degrees in IT fields. State officials reported that without the program, it was more likely their staff would leave for other agencies or the private sector.
- VA officials reported that the agency developed a program for skilled IT professionals within VA that might be interested in developing cloud computing skills. Groups of IT staff entered a 3-month rotation to learn cloud-related skills. VA officials said that the program had been very successful, and the agency had onboarded staff from the rotational program. Further, VA officials reported that they had created a working group of five agencies to work on incentivizing specific IT job series to increase pay rates. OPM approved the special salary rate in 2023,[191] and VA implemented the new rate the same year.[192] Finally, VA offered sign-on bonuses to help with recruiting skilled IT staff for critical need areas such as cloud.

[190]We recently reported on SSA's IT acquisition staffing challenges and made recommendations to the agency to address them; SSA concurred with the recommendations. See GAO, *Social Security Administration: Actions Needed to Address IT Acquisition Workforce Challenges*, GAO-25-107437 (Washington, D.C.: Aug. 14, 2025).

[191]OPM approved a special salary rate for IT specialists in the General Schedule-2210 series in 2023. A special salary rate is a pay-setting authority approved by OPM to provide higher rates of basic pay for specific general schedule positions in designated geographic areas, addressing recruitment and retention challenges. The General Schedule-2210 series positions are administrative positions that manage, supervise, lead, administer, develop, deliver, and support IT systems and services.

[192]VA terminated the special salary rate for its IT workers in October 2025.

- SSA officials reported that they developed an acquisition academy model to address shortfalls in procurement staff. SSA officials reported that the agency recruited college graduates for contracting officer roles and provided them with training and other on-the-job opportunities to grow their expertise.

GSA FAS officials stated that GSA had undertaken a variety of activities to support procurement training and workforce across the federal government. This included establishing a community of practice that had trained approximately 3,000 people on cloud procurement and infrastructure, with multiple requested trainings on cloud operations. The officials also described the work that the agency's previous office had performed to help agencies address this workforce problem, including providing team members to provide agencies with guidance on cloud acquisitions.[193]

GSA FAS officials stated that GSA and the CIO Council were developing guidance for agencies that would address cloud training needs. GSA's and the CIO Council's efforts to produce guidance for agencies on cloud acquisitions can provide a useful resource for agencies to use for training cloud staff.

Conclusions

To help inform cloud decisions, agencies have relied on and used historical procurement data. However, federal agency contract data lacked precision because only one code was permitted to be entered into the federal procurement data system. These data quality issues are not new—agencies have struggled for decades with the reliability of these data. Timely implementation of the many recommendations GAO has made to federal agencies to improve these data could result in high-quality information.

The FAR is severely out of date on cloud-related definitions. It does not include a definition of a commercial product or commercial service that would align with cloud services. Further, its definition of IT, rooted in a 1996 statute, is not consistent with the OMB definition of IT from the 2014 enactment of FITARA and it does not have a definition of cloud computing at all. Legislative action to modernize and include the definition of IT and cloud computing, respectively, would assist federal agencies in taking

[193]Since 2014, GSA had used its former digital consulting office, called 18F, to partner with agencies to build, buy, and share technology products. Multiple agencies in our review reported that this support helped them to overcome some of their workforce challenges. GSA eliminated the office in March 2025.

advantage of consumption-based solutions such as cloud services to help transform the federal IT landscape.

Other challenges also hamper federal agencies' pursuit of cloud solutions. Agencies continued to struggle with managing their cloud costs. GSA's FinOps pilots demonstrated that agencies could optimize their cloud environments to improve service operability, increase security, and identify cost savings. Expanding the FinOps framework across the federal government could lead to substantial cost savings.

Further, conflicting OMB and NIST guidance on the data collection and storage for software bill of materials create unnecessary burdens for agencies pursuing cloud solutions. CISA is well positioned to remedy this conflict by providing additional guidance on SBOM implementation to agencies.

In using multiple cloud providers, several agencies are achieving additional efficiencies but also running into new challenges such as interoperability. Sharing multi-cloud leading practices would enable agencies to learn from each other and improve implementation efforts.

Matters for Congressional Consideration

We are recommending the following two matters for congressional consideration:

Congress should consider: 1) updating the statutory definitions of commercial products and commercial services, and (2) requiring acquisition regulations be updated to reflect these definitions. (Matter for Consideration 1)

Congress should consider requiring acquisition regulations be updated to (1) define information technology to be consistent with the definition in FITARA and (2) define the term cloud computing to be consistent with the National Institute of Standards and Technology's definition. (Matter for Consideration 2)

Recommendations for Executive Action

We are making three recommendations—one to GSA, one to DHS, and one to the Federal CIO Council.

The Administrator of General Services, as the Executive Agent in charge of all government-wide IT acquisition contracts, should require agencies to use FinOps practices and report the extent of benefits resulting from the use of the practices. (Recommendation 1)

The Secretary of Homeland Security should direct the Director of the Cybersecurity and Infrastructure Security Agency to issue additional SBOM implementation guidance to agencies. This should include information on how agencies should integrate SBOM generation, consumption, and analysis into their risk management, purchasing, and software development practices, and how to leverage tools where appropriate. (Recommendation 2)

The Federal CIO Council, working with its chair, the Office of Management and Budget's Deputy Director for Management, should collect and share examples of leading practices in the federal government on multi-vendor cloud solutions, including containerization and testing platform interoperability. (Recommendation 3)

Agency Comments and Our Evaluation

We provided a draft of this report to OMB, including the CIO Council, and the 24 Chief Financial Officers Act agencies for their review and comment. Of the three agencies that we made recommendations to, DHS provided written comments and agreed with our recommendation and GSA provided written comments and disagreed with our recommendation. The CIO Council did not provide comments on our recommendation and OMB did not provide comments separate from the CIO Council.

DHS concurred with our recommendation. In written comments from DHS, reprinted in Appendix II, DHS's Director of Financial Management stated that CISA, led by the Cybersecurity Division, was currently updating its guidance related to the minimum elements for a SBOM. The agency noted that these requirements would support SBOM adoption and implementation by establishing shared expectations for bill of material data. In addition, the guidance was intended to support agencies in integrating bill of material generation, consumption, and analysis into software risk management, acquisition, purchasing, and software development practices. The agency estimated that the guidance would be completed by September 30, 2026. DHS also provided technical comments, which we addressed as appropriate.

GSA disagreed with our recommendation. In its written comments, reprinted in Appendix III, the Administrator of General Services stated that the agency did not have the authority to mandate that agencies use FinOps practices. The agency stated that FinOps was not an acquisition challenge but rather a framework that could be adopted widely and had been successfully piloted by several agencies. GSA noted that its IT

contracts could be used by agencies to procure products, services, and solutions supporting FinOps practices.

However, the President granted GSA this authority under Executive Order 14240, issued in March 2025.[194] Specifically, the Administrator of General Services was designated the executive agent in charge of all government-wide IT acquisition contracts in order to eliminate waste and duplication across the federal government. Further, OMB memorandum M-25-31 designated GSA with responsibility for the reduction of redundant and inefficient procurement activity within IT contracts, including cloud contracts.[195] As a result, GSA became the centralized contracting authority for the federal government, tasked with standardizing procurement practices to drive cost efficiency across the agencies.

Our report noted that 17 agencies faced challenges managing cloud costs after migrating from on-premise systems and across diverse environments. We share GSA's view that FinOps is a solution rather than an acquisition challenge. If properly implemented, FinOps can help federal agencies control cloud expenditures while advancing GSA's goal to reduce redundant and inefficient procurement within IT contracts. Consequently, we maintain our recommendation is warranted. In addition, GSA provided technical comments, which we incorporated as appropriate.

In addition, of the 22 agencies we did not make recommendations to, three agencies (DOD, SBA, and SSA) provided written comments on the draft report. One agency (SSA) stated that it believed that it would benefit from the recommendations made in the report. The other two agencies (DOD and SBA) stated that they had concerns regarding the information presented in the report. Specifically, both agencies indicated that we should have provided more granularity regarding specific cloud-related topics, as the agencies thought that oversimplification could lead to statements that would be imprecise or inaccurate.

- In written comments from SSA, reprinted in appendix IV, the Chief Risk Officer for SSA stated that the agency would benefit from

[194]Exec. Order No. 14240, *Eliminating Waste and Saving Taxpayer Dollars by Consolidating Procurement* (March 20, 2025).

[195]Office of Management and Budget, M-25-31.

updates to the FAR, the expansion of the FinOps framework, and a standard software bill of materials and central repository.

- In written comments from DOD, reprinted in Appendix V, the Acting Deputy Chief Information Officer for Information Enterprise stated the report represented a substantial and well-researched body of work that addressed issues of genuine importance to federal information technology modernization. While the report did not contain recommendations directed to the DOD, the department stated that it had identified areas where the report's current framing contained factual inaccuracies, omitted critical context, or could lead agencies to misinterpret key concepts and adopt suboptimal strategies.

    - The department stated that we characterized "vendor lock-in" as an inherently negative condition, which was oversimplified and inconsistent with current cloud strategy best practices. DOD stated that leveraging provider-specific capabilities was often the strategically correct decision, provided the agency maintained architectural awareness of its dependencies and had a documented exit strategy for mission-critical workloads. The department recommended that we reframe the discussion to advise agencies to "manage vendor concentration risk" rather than "avoid vendor lock-in."

      As discussed in the report, avoiding vendor lock-in when designing an overall cloud strategy is consistent with current federal cloud guidance. This includes OMB's *Federal Cloud Smart Strategy*,[196] the CIO Council's *Cloud Operations Best Practices and Resources Guide*,[197] the National Security Telecommunications Advisory Committee's *Report to the President on Zero Trust and Trusted Identity Management*,[198] and NIST's Special Publication 800-146,[199] among others. However, we also discuss agency procurements of niche cloud technologies from limited vendors, which could naturally lead to vendor lock-in

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

[197]General Services Administration and CIO Council, *Cloud Operations Best Practices and Resources Guide* (Oct. 2023).

[198]The President's National Security Telecommunications Advisory Committee, *NSTAC Report to the President: Zero Trust and Trusted Identify Management* (Feb. 23, 2022)

[199]National Institute of Standards and Technology, *Cloud Computing Synopsis and Recommendations*, Special Publication 800-146 (Gaithersburg, MD: May 2012).

in those cases. We agree that agencies should ensure their procurements are driven by an evaluation of the relevant risks, consistent with NIST's *Risk Management Framework*.[200]

- The department stated that we used the term "multicloud" generically without consistently scoping the discussion to the appropriate cloud service models. While DOD noted that our background section discussed multi-cloud within the context of IaaS offerings, we did not refer to IaaS in later discussions of multi-cloud in the report. The department stated that this omission could lead agencies to misinterpret the guidance as suggesting that multi-vendor strategies were viable with SaaS applications for a single business function, which would be infeasible and expensive.

  Our report includes essential background information on multi-cloud environments, as well as a discussion of relevant cloud service models. The finding sections focus on our analytical results rather than repeating previously stated background facts. We also made the recommendation to the CIO Council at a high level to allow the Council to have flexibility in developing the appropriate guidance. However, while we believe the language in the section is sufficiently clear, we clarified the section with a footnote to ensure no other agency experiences similar confusion.

- The department stated that we gave containerization and container orchestration tools disproportionate prominence as multi-cloud enablers in the report. DOD stated that we should address other topics related to multi-cloud architecture decisions, including data gravity, egress costs, and provider-specific managed service implementations.

  Our report's discussion on multi-cloud challenges focused primarily on containerization and orchestration platforms because these were the topics highlighted by the 17 agencies—including DOD—during our interviews and subsequent requests for clarification. We acknowledge other multi-cloud factors exist, but

[200]National Institute of Standards and Technology, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, Special Publication 800-37 Rev. 2 (Gaithersburg, MD: Dec. 2018).

because they were not raised by the agencies, they were not included in the report.

- The department stated that the SBOM discussion did not distinguish between cloud software products (that agencies install and manage) and managed cloud services (that agencies consume), where use of an SBOM would or would not be actionable.

  Our report evaluates the challenge of implementing OMB's SBOM guidance as this was the primary concern raised by all 17 agencies in our review. We have revised the SBOM section to incorporate other technical comments regarding how agencies should utilize SBOM data and technical tools. We believe these revisions should resolve the department's concern.

- The department stated that our report presented FedRAMP vendor and agency complaints largely at face value without critically examining the source of cited delays and costs. DOD recommended that the report disaggregate costs, correctly attribute delays between provider-controlled and government-controlled process steps and distinguish between the cost of the authorization process and the cost of achieving an adequate security posture. In addition, the department noted that it supported modernization efforts that addressed the government review portion of the process.

  Our report assessed the FedRAMP issues reported by the 15 agencies during our interviews and subsequent follow-up. We also included FedRAMP program cost data reported by agencies and vendors from other prior work because the data supported the issues identified.[201] As detailed in the report, FedRAMP 20x is intended to streamline and automate authorization processes, making a key improvement to the program once it is fully implemented. We modified the section to incorporate other technical comments to include more details on FedRAMP 20X activities. Consequently, we believe this section sufficiently captures the 15 agencies' positions and ongoing program efforts.

[201]See GAO-24-105691.

DOD also provided technical comments, which we addressed as appropriate.

- In written comments from SBA, reprinted in Appendix VI, the Deputy Chief Information Officer for SBA provided additional information regarding the agency's use of cloud procurement data and how the agency used it to inform decision-making. We updated our assessment to reflect this information.

  In addition, SBA agreed with the report's assessment that improvements in procurement data quality, centralized acquisition management, and modernization of the FAR were important enablers of more effective and efficient cloud adoption. The agency also stated the report's emphasis on enhanced cost management practices, harmonization of guidance, and the sharing of best practices across agencies provided value.

  The agency also suggested that future GAO work consider placing greater emphasis on enterprise architecture, interoperability, and technical standards as complementary drivers of cloud effectiveness. SBA stated that, in the agency's experience, long-term cost control, cybersecurity resilience, and cross-agency collaboration depended not only on how cloud services were acquired, but also on the consistency of identity management, data exchange frameworks, security architectures, and platform integration models. Accordingly, the agency stated that it believed that incorporating additional analysis and recommendations related to government-wide reference architectures, identity federation models, interoperability standards, and shared technical services could further strengthen the report and enhance its practical value to federal agencies.

  We share SBA's view that these topics are important for the effectiveness of federal cloud services. Although this review prioritized cloud procurement, our broader portfolio of information technology and cybersecurity work examines topics in these areas.

In addition, of the remaining 19 agencies that did not receive recommendations, 18 agencies did not provide comments on the draft report (Agriculture, Commerce, Education, Energy, EPA, HHS, HUD, Interior, Justice, Labor, NASA, NRC, NSF, OPM, State, Transportation, Treasury, and VA). USAID was also unable to provide comments because staff from the agency's Office of the Executive Secretariat reported that other agency needs had taken priority. Further, of these

agencies, we also received technical comments from three agencies, which we have incorporated as appropriate.

We are sending copies of this report to the appropriate congressional committees, the Administrator of General Services, 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 harriscc@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 VII.

//SIGNED//

Carol C. Harris
Director, Information Technology
and Cybersecurity

Appendix I: Objectives, Scope, and Methodology

Our objectives were to: (1) assess the cloud procurement data that agencies and the Office of Management and Budget (OMB) collect and use to inform decision-making on cloud acquisitions, (2) identify agency leading practices for procuring cloud services and any government-wide efforts to adopt the practices, and (3) assess agency cloud procurement challenges and government-wide efforts to address the challenges.

To address these objectives, we selected the 24 covered agencies for this review because these agencies were all required to implement Cloud Smart.[1] These agencies were the Department of Agriculture, Department of Commerce, Department of Defense (DOD), Department of Education, Department of Energy, Department of Health and Human Services (HHS), Department of Homeland Security (DHS), Department of Housing and Urban Development (HUD), Department of the Interior, Department of Justice, Department of Labor, Department of State, Department of Transportation, Department of the Treasury, Department of Veterans Affairs (VA), Environmental Protection Agency (EPA), General Services Administration (GSA), National Aeronautics and Space Administration (NASA), National Science Foundation (NSF), Nuclear Regulatory Commission (NRC), Office of Personnel Management (OPM), Small Business Administration (SBA), Social Security Administration (SSA), and the U.S. Agency for International Development (USAID).

Analyzing Agencies' Use of Cloud Procurement Data

To address the first objective, we analyzed agencies' documentation describing the use of cloud procurement data and descriptions of cloud procurement data key practices. This included documentation such as agencies' cloud strategies, road maps, cloud procurement and security-related guidance, contract clauses, as well as related directives.

We also analyzed cloud obligated spending data from the Federal Procurement Data System (FPDS). We assessed the reliability of the FPDS cloud data because OMB stated that it used these data to make decisions regarding cloud procurements. This included the 24 agencies'

[1]The term covered agency refers to the 24 major agencies listed in the Chief Financial Officers Act of 1990. 31 U.S.C. § 901(b).

use of cloud services data for fiscal year 2022.[2] We chose to begin with fiscal year 2022 because that was the fiscal year of data that was most recently available at the time we began our review. We excluded all contract actions with contracting agencies other than the 24 agencies. In addition to the contracting agency, the FPDS data included the contract and order identification numbers, business name, obligation amounts by year, the award description, and product and service code (PSC) information.

Reliability of Federal Procurement Data System Data

We took the following steps to help determine the reliability of the data we collected. First, we analyzed the PSC manuals for June 2019 and October 2020 to determine a list of relevant cloud-related PSCs for those fiscal years.[3] We took this step because, in 2020, OMB had led efforts to modernize IT PSCs, and the codes were updated to include additional ones for capabilities delivered "as a service" (cloud computing). In addition, an agency could have begun cloud procurement under an earlier PSC and still be obligating funds in fiscal year 2022 or 2023.[4] We also reviewed a list of cloud-related PSCs on GSA's Cloud Computing and Cloud Related IT Professional Services website. We then compiled a list of eight cloud-related codes.

- **Business application and application development software as a service (DA10):** This includes support services, delivered as a service contract (software as a service or subscription) involved with the analysis, design, development, code, test and release packaging services associated with application development projects, as well as off-the-shelf business software.

[2]Prior to February 24, 2026, the Federal Procurement Data System (FPDS) was the federal government's central database of information on federal procurement actions. Through the *Office of Federal Procurement Policy Act of 1974*, Congress mandated that contract actions using appropriated funds must be reported to FPDS, the central repository of information on federal contracting. FPDS was managed by General Services Administration (GSA). On February 24, 2026, GSA retired the FPDS.gov website and its ezSearch tool, migrating all federal procurement data into the System for Award Management (SAM.gov). SAM.gov is an integrated award environment hosted by GSA. The site is now the centralized platform for this data.

[3]General Services Administration, *Federal Procurement Data System Product and Service Codes (PSC) Manual, Fiscal Year 2021 Edition* (Oct. 30, 2020); and *Federal Procurement Data System, Product and Service Codes Manual, June 2019 Edition* (June 28, 2019).

[4]The original PSC for cloud computing was IT and Telecom—Teleprocessing, Timeshare, Cloud Computing, and High Performance Computing (D305).

- **Compute as a service (mainframes/servers) (DB10):** This includes computing delivered as a service in a public or private cloud environment such as services for traditional mainframe computers and operations running various operating systems.
- **Data center as a service (DC10):** This includes data center services delivered as a service contract and offsite data center facilities using the resources provided by third parties. It may be part of an infrastructure as a service offering.
- **End user as a service (DE10):** This includes support services for end user client computing delivered as a service contract, including providing service desk, workspace technical support, conferencing, and printer support. Workspace support can include desktop as a service and workspace as a service delivered by public cloud or third-party providers. It can also include client-related software accessed as a service used to author, create, collaborate and share documents and other content.
- **IT management as a service (DF10):** This includes management tools and services delivered as a service, by subscription, or as a service contract.
- **Network as a service (DG10):** This includes network services delivered as a service, by subscription, or as a service contract, network services delivered in connection with other infrastructure as a service and platform as a service, cloud-based network management services, and software defined networks accessed by service contract or subscriptions.
- **Platform as a service (DH10):** This includes platform delivered as a service for databases and middleware, and mainframe database and middleware delivered as a service.
- **Storage as a service (DK10):** This includes cloud solutions delivered as a service and mainframe storage as a service.

Second, we reviewed the compiled list of each agency's cloud-related contracting actions with obligated amounts for fiscal year 2022 to identify missing data or other errors. We consulted with our data quality expert about these issues as appropriate. In addition, we provided a copy of the list of cloud-related contracting actions to each agency. We asked each agency to confirm that the list of contracts and the total amount obligated by each agency for cloud services for fiscal year 2022 was correct.

Sixteen agencies reported issues with the data. Specifically, 13 agencies reported issues with the PSCs, including that a PSC reflected a service other than cloud because cloud services were a secondary purchase. In addition, two agencies reported that their spreadsheets included contracts

where the PSC had been allocated incorrectly; one agency reported that FPDS would be updated for those contracts while the other agency did not specifically state plans to do so. Further, five agencies reported that they were unable to validate the data in the spreadsheets we provided to their agency. We reviewed the updated information and other agencies' qualifications of the provided data and followed up with agency officials to clarify the responses as appropriate.

We presented the results of our analysis of the FPDS data to each of the 24 agencies. We asked the agencies to verify the completeness and accuracy of these data and provide any updates as appropriate. All 24 agencies confirmed the data or provided updated information. Based on our assessment of the data and the measures that we took to assess the reliability of the data reported in FPDS, we determined that FPDS cloud data were not sufficiently precise for reporting aggregated cloud spending. We therefore did not include the obligated cloud contract spending amounts in our report. In addition, we discuss the issues with the impreciseness of data in the report.

Our analysis of FPDS data was conducted prior to the migration of the system into SAM.gov in February 2026. For the purpose of this report, we discuss the FPDS policies that were current as of February 2026 because these were in place when we conducted our audit work with the 24 agencies in our review.

We also determined that the control activities component and information and communications component of internal control were significant to this objective. This included the underlying principles that management should design the entity's information system and related control activities to achieve objectives and respond to risks; implement control activities through policies; use quality information (information that is appropriate, current, complete, and accurate) to make informed decisions and achieve its objectives; and externally communicate the necessary quality information to achieve the entity's objectives. We analyzed the 24 agencies' responses to questions regarding cloud data, the information system(s) that produced the data, and agency descriptions of steps taken to ensure data reliability, along with supporting documentation. We also reviewed relevant prior GAO or Office of Inspector General work that assessed the selected agencies' IT data, as appropriate. We determined whether the 24 agencies had ensured their information processing objectives (accuracy and completeness) were met. We also evaluated the sources of data for reliability to ensure the data was reasonably free from

error, as noted in the *Standards for Internal Control in the Federal Government*.[5]

We also interviewed knowledgeable senior officials from each of the 24 agencies from the offices of the Chief Information Officer (CIO), the Senior Procurement Executive, the Chief Acquisition Officer, the Chief Financial Officer, and other components in charge of cloud services. We sought information regarding their agency's use of cloud procurement data and the decisions made using these data. Further, we interviewed staff from OMB's Office of the Federal CIO and Office of Federal Procurement Policy (OFPP).

Assessing Agency Procurement Practices and Challenges

To address the second and third objectives, we interviewed knowledgeable senior officials from each of the 24 agencies from the offices of the CIO, the Senior Procurement Executive, the Chief Acquisition Officer, the Chief Financial Officer, and other components in charge of cloud services regarding their agency's procurement practices and challenges.

To develop a list of topic areas for objective two for these meetings, we reviewed (1) prior GAO reports on cloud computing and procurement,[6] (2)

[5]GAO, *Standards for Internal Control in the Federal Government*, GAO-25-107721 (Washington, D.C.: May 15, 2025).

[6]GAO, *Federal Buying Power: OMB Can Further Advance Category Management Initiative by Focusing on Requirements, Data, and Training*, GAO-21-40 (Washington, D.C.: Nov. 30, 2020); *Information Technology, Selected Federal Agencies Need to Take Additional Actions to Reduce Contract Duplication*, GAO-20-567 (Washington, D.C.: Sept. 30, 2020); *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); *Cloud Computing: Agencies Have Increased Usage and Realized Benefits, but Cost and Savings Data Need to be Better Tracked*, GAO-19-58 (Washington, D.C.: Apr. 4, 2019); *Cloud Computing: Agencies Need to Incorporate Key Practices to Ensure Effective Performance*, GAO-16-325 (Washington, D.C.: Apr. 7, 2016); *Cloud Computing: Additional Opportunities and Savings Need to Be Pursued*, GAO-14-753 (Washington, D.C.: Sept. 25, 2014): and *Information Technology Reform: Progress Made but Future Cloud Computing Efforts Should be Better Planned*, GAO-12-756 (Washington, D.C.: July 11, 2012).

guidance from OMB, the CIO Council,[7] GSA,[8] and the Cybersecurity and Infrastructure Security Agency,[9] (3) laws and regulations, and (4) procurement processes for cloud service acquisition, workforce, and contracts for cloud services,[10] to identify leading procurement practices. We synthesized the information to develop a list of 16 topic areas that aligned with all the activities in a federal competitive acquisition process.[11]

During meetings with agency officials in the Office of the CIO, Office of the Senior Procurement Executive, Office of the Chief Acquisition Officer, Office of the Chief Financial Officer, and other components in charge of cloud services, we discussed with senior officials whether they had identified any specific leading practices for procuring cloud services in the areas identified. Because these 16 areas might not represent all potential

[7]This included guidance from the Chief Information Officer (CIO) Council's Federal Technology Investment Management Community of Practice.

[8]This included guidance from General Services Administration's (GSA) Cloud Adoption Center of Excellence, Cloud Information Center, and Cloud and Infrastructure Community of Practice. The Cloud Adoption Center of Excellence provides guidance and supports cloud implementation through a developed set of services based on best practices and successful uses cases, both in the commercial and government sectors. "Cloud Adoption," IT Modernization Centers of Excellence, General Services Administration, accessed on July 11, 2025. https://coe.gsa.gov/coe/cloud-adoption.html. "Cloud Information Center," OMB and CIO Council, last accessed on July 9, 2025. https://cic.gsa.gov.

[9]Cybersecurity and Infrastructure Security Agency, United States Digital Service, and Federal Risk and Authorization Management Program, *Cloud Security Technical Reference Architecture*, Version 2.0 (June 2022).

[10]This included guidance from GSA's Cloud Information Center. "Helping Government get on the Cloud," OMB and CIO Council, last accessed on July 9, 2025. https://cic.gsa.gov.

[11]The sixteen areas included: federal or agency procurement guidance, laws, and regulations; roadmap for cloud procurement, availability of information for requirements determination (functional, technical, security, hardware) and goal setting; scope determination; as-is and target architecture (single cloud vs. hybrid model); resources (e.g. financial, market research); procurement processes for cloud service acquisition; cloud acquisition workforce (hiring and retention, subject matter expertise, and training); cloud contracts (contract development, types of contracts [fixed price vs. time and materials], funding options for multi-year contracts, planning for fees [e.g. data egress]; cloud service provider (CSP)/vendor management (vetting new vendors, vendor selection, opportunities for small businesses [contracting assistance programs] , and transitioning between vendors; restrictive software licenses; Federal Risk and Authorization Management Program; iterative governance processes; category management; cloud data metrics; and collaboration among agency stakeholders [acquisition and operations].

practices, we also asked officials to describe any additional practices not included in these areas.

In addition, as part of these meetings, we asked officials from these offices at each agency to identify any recommendations regarding steps that could be taken to adopt the practice government-wide. All 24 agencies provided examples of leading practices in one or more of the sixteen topics areas provided. In addition, several agencies also provided examples in areas not included in the list that we noted.

To develop the list of practices, we reviewed: (1) interview responses, (2) agency-provided cloud policies, guidance, and other process documentation, (3) federal leading practice guidance, and (4) prior related reports since 2010. We chose 2010 because that was the first year agencies were required to begin using cloud services.

Because of the open-ended nature of the 24 agencies' responses to our questions, we conducted a content analysis of the information we received to identify and summarize the information reported by the agencies during the interviews. We reviewed the information reported by the agencies and initially created groupings using the 16 topic areas that our prior research had identified. We also grouped the additional information reported by the agencies together based on commonalities such as purpose and capabilities, and summarized the areas reported. We discussed the groupings of the reported practices and reached agreement on the categories. We confirmed a list of three practices and totaled the number of agencies that reported each of these.

To confirm that we had accurately characterized the agency procurement practices, we presented the results of our analysis to the 24 selected agencies. All 24 agencies confirmed the information or provided updated information, which we have incorporated as appropriate.

We also interviewed OMB (Office of the Federal CIO and OFPP) and GSA (Office of Government-wide Policy and Federal Acquisition Service) staff. We sought information regarding the federal cloud procurement strategy and any planned or ongoing government-wide efforts to promote the three agency key practices.

To further address the third objective, we also reviewed prior GAO cloud computing and procurement reports, guidance from OMB, the CIO Council, GSA, and the Cybersecurity and Infrastructure Security Agency, laws and regulations, and procurement processes for cloud service

acquisition, workforce, and contracts for cloud services, to identify federal procurement challenges. Using the same approach as objective two, we developed a list of 16 topic areas that aligned with all the activities in a federal acquisition process for negotiated acquisitions (noted previously).

We interviewed knowledgeable senior officials at each of the 24 agencies from the offices of the CIO, the Senior Procurement Executive, the Chief Acquisition Officer, the Chief Financial Officer, and other components in charge of cloud services regarding the agency's procurement challenges. We discussed with senior officials if the agency had identified challenges in the 16 areas discussed previously or had other procurement challenges.

To develop the list of challenges, we reviewed the content analysis of the interview responses, prior GAO reports since 2010, as well as agency-provided cloud policies, guidance, and other documentation on challenges such as presentations and lessons learned. In addition, recognizing that certain challenges identified could potentially impact most or all 24 federal agencies, we determined that we would reach out to the remaining agencies (who had not raised those issues) to find out whether officials at those agencies would also consider the issues to be a challenge. These included challenges associated with the Federal Acquisition Regulation (FAR), secure software development practices, managing IT cloud costs, multi-vendor cloud solutions, and the Federal Risk and Authorization Management Program (FedRAMP). We summarized each challenge and asked each agency whether they considered it a challenge. The additional agency responses received were incorporated into the analysis as appropriate. We confirmed a list of six challenges and totaled the number of agencies that reported each of these.

We also interviewed officials with OMB (Office of the Federal CIO and OFPP), and GSA (Office of Government-wide Policy, Federal Acquisition Service, and the Project Management Office for FedRAMP).

For the purposes of this report, we discuss the FAR policies and procedures that were current before the FAR was overhauled, using the March 2025 version of the federal regulation. We chose March 2025 because these regulations were in place when we conducted our audit work with the 24 agencies in our review. Significant changes to the FAR

were made between April 2025 and October 2025.[12] We therefore reviewed the FAR changes for the agency challenge on outdated IT regulations to determine whether the changes had addressed the areas noted in the challenges. We discuss these changes to the FAR as of October 2025 in the report. As such, for the purposes of this report, we refer to the March 2025 version as the FAR (legacy), and the Revolutionary FAR Overhaul version of October 2025 as the FAR (deviation). In addition, where relevant, we address the sections of the FAR (legacy) that have been updated pursuant to the Revolutionary FAR Overhaul (deviation).

We conducted this performance audit from April 2024 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[12]In April 2025, the President issued Executive Order 14275, which called for OMB and the FAR Council to amend the FAR by October 2025 so that it contained only provisions required by statute or that were otherwise necessary for sound procurement. The order also called for consistency and alignment of agency supplemental regulations and internal guidance with the changes made to the FAR. See Exec. Order No. 14275, *Restoring Common Sense to Federal Procurement*, 90 Fed. Reg. 16447 (Apr. 15, 2025).

Appendix II: Comments from the Department of Homeland Security

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

Homeland Security

BY ELECTRONIC SUBMISSION

June 1, 2026

Carol C. Harris
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548-0001

Re: Management Response to GAO-26-107530, "CLOUD COMPUTING: Federal Government Needs to Address Procurement Challenges"

Dear Ms. Harris:

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 (hereafter referred to as "the auditors") work in planning and conducting its review and issuing this report.

DHS leadership is pleased to note the auditors' positive recognition that four agencies included in the auditors' review reported that their facilitation of contract development benefited by using DHS' Procurement Innovation Laboratory to improve the efficiency of their cloud acquisition processes. The auditors noted that DHS established the Procurement Innovation Laboratory in March 2015 to experiment with innovative technologies for increasing efficiency in the procurement processes and institutionalizing best practices. Specifically, U.S. Department of Education officials stated that using the Procurement Innovation Laboratory saved 15 days in the source selection process, and U.S. Department of the Treasury senior officials stated that the Procurement Innovation Laboratory aided the agency in tracking contracts, monitoring protest rates, and gathering key acquisition data.

It is also important to highlight the Department's efforts to address procurement challenges with cloud computing and Software Bill of Materials technologies. Through

the implementation of its enterprise-wide Cumulus cloud procurement vehicles,[1] the Department demonstrated significant improvement in issuing and setting up policies, roles, and processes around cloud guidance, obtaining cloud solutions, enabling new cloud capabilities, and controlling cloud costs. Additionally, in September 2025, the Cybersecurity and Infrastructure Security Agency (CISA) released guidance[2] on Software Bill of Materials that allowed agencies to significantly reduce the time required to identify and respond to vulnerabilities. CISA also recently collaborated with the Office of Management and Budget to clarify and align existing Software Bill of Materials guidance and recommendations with Presidential Executive Order 14028[3] and National Institute of Standards and Technology guidance. DHS remains committed to addressing procurement challenges with cloud computing and Software Bill of Materials technologies which support the critical services the Department provides to the nation.

The draft report contained three recommendations, including one for DHS with which the Department concurs. Enclosed find our detailed response to this recommendation. DHS previously submitted technical comments addressing several accuracies, contextual, and other issues under a separate cover for the auditors' consideration, as appropriate.

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,

JEFFREY M BOBICH

Digitally signed by JEFFREY M BOBICH
Date: 2026.06.01 10:28:55 -04'00'

JEFFREY M. BOBICH
Director of Financial Management

Enclosure

[1] DHS Cumulus is an enterprise-wide cloud acquisition strategy designed to centralize and streamline how the department procures commercial Anything-as-a-Service. It primarily relies on a mix of competitive and non-competitive Indefinite-Delivery, Indefinite-Quantity vehicles, awarding direct contracts to hyperscale Cloud Service Providers.

[2] 2025 Minimum Elements for a Software Bill of Materials (SBOM)," dated August 22, 2025; See: https://www.cisa.gov/resources-tools/resources/2025-minimum-elements-software-bill-materials-sbom

[3] Executive Order 14028, "Improving the Nation's Cybersecurity," dated May 12, 2021; 86 FR 26633; See: https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity.

Enclosure: Management Response to Recommendation Contained in GAO-26-107530

GAO recommended that the Secretary of Homeland Security direct the CISA Director to:

Recommendation 2: Issue additional [Software Bill of Materials] implementation guidance to agencies. This should include information on how agencies should integrate [Software Bill of Materials] generation, consumption, and analysis into their risk management, purchasing, and software development practices, and how to leverage tools where appropriate.

Response: Concur. CISA, led by the Cybersecurity Division, is currently updating the Software Bill of Materials Minimum Elements, which includes the baseline technical requirements for a Software Bill of Materials. These requirements support Software Bill of Materials adoption and implementation by establishing shared expectations for Software Bill of Materials data and are intended to support agencies in integrating Software Bill of Materials generation, consumption, and analysis into software risk management, acquisition, purchasing, and software development practices. CISA is co-authoring the Software Bill of Materials Minimum Elements with international cybersecurity partner agencies to harmonize requirements for Software Bill of Materials globally.

The updated technical requirements will reflect current Software Bill of Materials needs, while preserving the core principles of the version published in 2021 by the National Telecommunications and Information Administration.[4] Increased adoption and implementation across stakeholders in the software ecosystem has uncovered new use cases and applications for Software Bill of Materials data. Software Bill of Materials tooling, in response to the increased adoption and implementation of Software Bill of Materials, has matured since 2021. These advancements enable organizations, including federal agencies requesting Software Bill of Materials, to demand more information about their software components and supply chain.

Updating the Software Bill of Materials Minimum Elements document is a product of two years of collaboration with cybersecurity experts and practitioners across the software ecosystem. On August 22, 2025, CISA published a Request For Information in the Federal Register to solicit public comment on the updated draft of the Software Bill of Materials Minimum Elements.[5] After careful review of the public comments, CISA

[4] "The Minimum Elements For a Software Bill of Materials (SBOM)," dated July 12, 2021; See: https://www.ntia.gov/sites/default/files/publications/sbom_minimum_elements_report_0.pdf.
[5] "Request for Comment on 2025 Minimum Elements for a Software Bill of Materials," dated August 22, 2025; 90 FR 41094; See: https://www.federalregister.gov/documents/2025/08/22/2025-16147/request-for-comment-on-2025-minimum-elements-for-a-software-bill-of-materials.

updated the draft and solicited feedback from international peer cybersecurity agencies in quarter 1 of fiscal year 2026. Following the completion of required internal reviews, the final version will be published by the end of fiscal year 2026.

Estimated Completion Date (ECD): September 30, 2026.

Appendix III: Comments from the General Services Administration

U.S. General Services Administration

March 18, 2026

Orice Williams Brown
Acting Comptroller General of the United States
U.S. Government Accountability Office
Washington, DC 20548

Dear Acting Comptroller General Brown:

The U.S. General Services Administration (GSA) appreciates the opportunity to review and comment on the U.S. Government Accountability Office (GAO) draft report, Cloud Computing: Federal Government Needs to Address Procurement Challenges (GAO-26-107530).

GAO made the following recommendation to GSA:

> The Administrator of General Services, as the Executive Agent in charge of all government-wide IT acquisition contracts, should require agencies to use FinOps practices and report the extent of benefits resulting from the use of the practices. (Recommendation 1)

GSA does not agree with the recommendation.

> Per the FinOps Foundation (https://www.finops.org/introduction/what-is-finops/), "FinOps is an operational framework and cultural practice which maximizes the business value of cloud and technology, enables timely data-driven decision making, and creates financial accountability through collaboration between engineering, finance, and business teams. (FinOps Foundation Technical Advisory Council, January 2025)." FinOps is not an acquisition challenge but rather a framework that can be adopted widely and has been successfully piloted by several agencies.
>
> GSA does not have the authority to mandate that agencies use FinOps practices; however, GSA IT contracts can be used by agencies to procure products, services, and solutions supporting FinOps practices, which can improve agencies' real-time cloud management.

We suggest the audit recommendation be changed to the following language:

> The Administrator of General Services should promote best practices over the next 12 months to support FinOps adoption and maturity for interested federal agencies.

1800 F Street NW
Washington DC 20405-0002
www.gsa.gov

If you have any questions or require additional information, please contact Mark O'Connell, Associate Administrator, GSA Office of Congressional and Intergovernmental Affairs, at GSACongressionalAffairs@gsa.gov.

Sincerely,

Edward C. Forst
Administrator

Enclosure

cc: Carol C. Harris, Director, Information Technology and Cybersecurity, GAO

Appendix IV: Comments from the Social Security Administration

SOCIAL SECURITY
Office of the Commissioner

March 13, 2026

Carol C. Harris
Information Technology and Cybersecurity
United States Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Director Harris,

Thank you for the opportunity to review the draft report " CLOUD COMPUTING: Federal Government Needs to Address Procurement Challenges" (GAO-26-107530). We would benefit from updates to the Federal Acquisition Regulation, the expansion of FinOps framework, and a standard software bill of materials and central repository.

Please contact me at (410) 274-0654) if I can be of further assistance. Your staff may contact Amy Gao, Director of the Audit Liaison Staff, at (410) 966-1711.

Sincerely,

Chad Poist
Chief Risk Officer

SOCIAL SECURITY ADMINISTRATION BALTIMORE, MD 21235-0001

Appendix V: Comments from the Department of Defense

CHIEF INFORMATION OFFICER

DEPARTMENT OF WAR
6000 Defense Pentagon
Washington, D.C. 20301-6000

Ms. Carol Harris
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Ms. Harris,

This is the Department of War (DoW) response to the GAO Draft Report, GAO-26-107530, "Cloud Computing: Federal Government Needs to Address Procurement Challenges," dated February 19, 2026 (GAO Code 107530).

The DoW appreciates the opportunity to review this draft report. The report represents a substantial and well-researched body of work that addresses issues of genuine importance to federal information technology modernization. While the report does not contain recommendations directed to the DoW, the Department has identified areas where the report's current framing contains factual inaccuracies, omits critical context, or could lead agencies to misinterpret key concepts and adopt suboptimal strategies.

The Department offers the following five comments, detailed in Enclosure 1, to strengthen the report's accuracy and ensure that its guidance drives sound decision-making across the federal enterprise:

Comment 1: Vendor Lock-In Framing: The report's characterization of "vendor lock-in" as an inherently negative condition is oversimplified and inconsistent with current cloud strategy best practices. The DoW recommends reframing the discussion to advise agencies to "manage vendor concentration risk" rather than "avoid vendor lock-in." Leveraging provider-specific capabilities is often the strategically correct decision, provided the agency maintains architectural awareness of its dependencies and has documented exit strategies for mission-critical workloads. The report's own discussion of the Department of Defense's multicloud strategy supports this distinction but does not draw it explicitly.

Comment 2: Multicloud Applicability Across Service Models: The report uses the term "multicloud" generically without consistently scoping the discussion to the appropriate cloud service models. While the background section correctly notes that multicloud generally refers to Infrastructure as a Service offering, this qualification is not carried into the findings or recommendations. This omission could lead agencies to misinterpret the guidance as suggesting that multi-vendor strategies are viable at the Software as a Service layer for a single business function — an approach that would be operationally infeasible, prohibitively expensive, and strategically incoherent.

Comment 3: Containerization and Multicloud Portability: The report gives containerization and container orchestration tools disproportionate prominence as multicloud enablers. While containerization provides a consistent compute orchestration layer, it does not address the more significant sources of vendor dependency at the managed services and data layers. The report should address data gravity, egress costs, and provider-specific managed service implementations as primary factors in multicloud architecture decisions.

Comment 4: Software Bills of Materials in Cloud Environments: The report does not distinguish between software products that agencies install and manage — where Software Bills of Materials are actionable — and managed cloud services that agencies consume — where the appropriate security assurance mechanism is outcome-based attestation through the Federal Risk and Authorization Management Program, continuous monitoring, and the provider's demonstrated ability to rapidly communicate and remediate vulnerabilities.

Comment 5: Federal Risk and Authorization Management Program Authorization: The report presents vendor and agency complaints about the Federal Risk and Authorization Management Program largely at face value without critically examining the source of cited delays and costs. The DoW recommends that the report disaggregate costs, correctly attribute delays between provider-controlled and government-controlled process steps and distinguish between the cost of the authorization process and the cost of achieving an adequate security posture. The Department supports modernization efforts that address the government review portion of the process.

Additionally, the Department identified factual inaccuracies regarding the Air Force Cloud One program that require correction. These technical comments are provided in Enclosure 2.

The DoW appreciates the GAO's thorough examination of federal cloud procurement challenges and welcomes the opportunity to discuss these comments further. The point of contact for this matter is Mr. Robert Vietmeyer, robert.w.vietmeyer.civ@mail.mil, (571) 372-4461.

Sincerely,

Carl D. Porter
Deputy Chief Information Officer
for Information Enterprise (Acting)

Enclosures:
1. DoW Detailed Comments on GAO Draft Report GAO-26-107530
2. DoW Technical Corrections to GAO Draft Report GAO-26-107530

Appendix VI: Comments from the Small Business Administration

April 3, 2026

Subject: Response to Draft GAO Report – GAO 26-107530

Dear Carol C. Harris,

Thank you for the opportunity to review and comment on the draft report entitled Cloud Computing: Federal Government Needs to Address Procurement Challenges (GAO-26-107530). We appreciate GAO's engagement with the agency and its continued focus on improving federal information technology management and acquisition practices.

Regarding footnote 75 on p. 31, I see in our audit tracking system that GAO split the Cloud Smart Procurement Implementation engagement into two engagements (106137 first, and then 107530), and perhaps our team lost track of the second engagement. The answer to the question is Yes, the SBA used cloud-related data to guide decision-making for cloud procurements by leveraging multiple sources of operational and financial information, including workload analysis, detailed billing data, and cost-explorer dashboards and portals, among other tools and reports. This data-driven approach enabled the agency to understand actual resource utilization, compare costs across environments and providers, and identify optimization opportunities before making procurement decisions. In addition, SBA used information from performance monitoring, security and compliance reporting, and data center consolidation metrics to further inform its strategies for selecting, scaling, and managing cloud services.

Overall, the agency agrees with the report's assessment that improvements in procurement data quality, centralized acquisition management, and modernization of the Federal Acquisition Regulation are important enablers of more effective and efficient cloud adoption. We also recognize the value of the report's emphasis on enhanced cost management practices, harmonization of guidance, and the sharing of best practices across agencies.

In addition, the agency respectfully suggests that future versions of this report, or related GAO work, consider placing greater emphasis on enterprise architecture, interoperability, and technical standards as complementary drivers of cloud effectiveness. In the agency's experience, long-term cost control, cybersecurity resilience, and cross-agency collaboration depend not only on how

cloud services are acquired, but also on the consistency of identity management, data exchange frameworks, security architectures, and platform integration models.

Without common architectural and interoperability standards, agencies may continue to experience fragmented environments, limited data sharing, and increased operational complexity, even under centralized or improved acquisition models. These challenges are particularly significant for small and mid-sized agencies with limited technical and integration resources.

Accordingly, the agency believes that incorporating additional analysis and recommendations related to government-wide reference architectures, identity federation models, interoperability standards, and shared technical services could further strengthen the report and enhance its practical value to federal agencies.

We appreciate the thoroughness of GAO's work and the opportunity to provide input on this important topic. Please let us know if you have any questions regarding these comments or if additional information would be helpful.

Sincerely,

DOUGLAS ROBERTSON

Digitally signed by DOUGLAS ROBERTSON
Date: 2026.04.03 10:11:25 -04'00'

Douglas Robertson
Deputy Chief Information Officer

Appendix VII: GAO Contact and Staff Acknowledgments

GAO Contact

Carol C. Harris, harriscc@gao.gov

Staff Acknowledgments

In addition to the individual named above, the following staff made key contributions to this report: Eric Winter (Assistant Director), Jon Ticehurst (Assistant Director), Guisseli Reyes-Turnell (Assistant Director), Valerie Hopkins (Analyst-in-Charge), Logan Arkema, Chris Businsky, Quade Bywater, Donna Epler, Rebecca Eyler, Suellen Foth, Amanda Gill, Lee Hinga, Michael Lebowitz, Lisa Maine, Philip Menchaca, Evan Nelson Senie, Christine Pecora, and Haley Weller.