CLOUD SECURITY

Federal Authorization Program Usage Increasing, but Challenges Need to Be Fully Addressed

Accessible Version

Report to Congressional Committees

January 2024
GAO-24-106591
United States Government Accountability Office

GAO Highlights

View GAO-24-106591. For more information, contact David B. Hinchman at (214) 777-5719 hinchmand@gao.gov.
Highlights of GAO-24-106591, a report to congressional committees

January 2024

CLOUD SECURITY

Federal Authorization Program Usage Increasing, but Challenges Need to Be Fully Addressed

Why GAO Did This Study

OMB established the FedRAMP program in 2011. Managed by GSA, FedRAMP aims to ensure that cloud services have adequate information security while also reducing operational costs. To accomplish this goal, FedRAMP established a standardized process for authorizing CSPs' cloud services.

The James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 includes a provision for GAO to review the status of the FedRAMP program. GAO's objectives were to identify (1) the frequency and types of services agencies have used under FedRAMP; (2) the amounts of costs incurred by selected agencies and CSPs in pursuing FedRAMP authorizations; and (3) the key challenges selected agencies and CSPs face in the authorization process and determine the extent to which GSA and OMB have taken actions to address them.

GAO analyzed questionnaire responses from six selected CFO Act agencies and 13 selected CSPs. GAO selected these agencies and CSPs based on several factors, including the number of authorizations agencies had sponsored, the authorization path used by the CSPs, and whether a CSP was a small business. GAO also reviewed GSA and OMB data and interviewed appropriate agency and CSP officials.

What GAO Recommends

GAO is making three recommendations, two to OMB and one to GSA, to finalize efforts to address challenges related to FedRAMP. GSA agreed with its recommendation and OMB did not comment on the recommendations.

What GAO Found

The Office of Management and Budget (OMB) established the Federal Risk and Authorization Management Program (FedRAMP) to provide a standardized approach for authorizing the use of cloud services. From July 2019 to April 2023, the 24 Chief Financial Officers (CFO) Act agencies increased the number of authorizations by about 60 percent. These authorizations covered services ranging from a basic computer infrastructure to a more full-service model that included software applications. OMB requires agencies to use FedRAMP. However, nine agencies reported they were using cloud services that were not FedRAMP authorized. OMB has not yet implemented GAO's recommendation to adequately monitor agencies' compliance with the program.

Selected agencies and cloud service providers (CSP) provided estimated costs when pursuing FedRAMP authorizations; data on actual costs were limited. 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 CSPs using varying methods to determine costs. A contributing factor to the varying methods was that OMB did not provide guidance on authorization costs to be tracked and reported. The lack of consistent cost data will also hamper OMB in determining whether its goal of reducing FedRAMP costs will be achieved.

The selected agencies and CSPs identified six key challenges that they faced in pursuing FedRAMP authorizations (see table).

Key Challenges Faced by Agencies and Cloud Service Providers (CSP) When Pursuing Federal Risk and Authorization Management Program (FedRAMP) Authorizations

Challenges	Description
Receiving timely responses from stakeholders	Agencies and CSPs reported that they had issues with receiving timely responses from stakeholders throughout the authorization process.
Sponsoring CSPs that were not fully prepared	Agencies reported that CSPs did not fully understand the FedRAMP process and lacked complete documentation.
Lacking sufficient resources	Agencies reported that they lacked the resources (e.g., funding and staffing) needed to sponsor an authorization.
Meeting FedRAMP technical and process requirements	CSPs reported that they had to update the infrastructure to meet federal security requirements.
Finding an agency sponsor	CSPs reported that finding an agency sponsor was difficult.
Engaging with third-party assessment organizations (3PAO)	CSPs reported that they faced issues (e.g., lack of consistency) when engaging with organizations that were responsible for performing independent assessments of their cloud servicesthe effort is not intended to address the identified challenge3PAOs.

Source: GAO analysis. | GAO-24-106591

In acknowledging these challenges, OMB and the FedRAMP program management office in the General Services Administration (GSA) already have efforts underway to address them. For example, OMB released proposed new FedRAMP guidance for public comment in October 2023. GSA also intends to, among other things, issue guidance on meeting certain technical requirements. However, OMB and GSA have not finalized these guidance documents or announced a schedule for doing so. As a result, agencies and CSPs may continue facing challenges, leading to additional costs to pursue authorizations.

Contents

Figures

Abbreviations

3PAO	third-party assessment organization
ATO	authority to operate
CFO	Chief Financial Officer
CSO	cloud service offering
CSP	cloud service provider
DHS	Department of Homeland Security
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standard
GSA	General Services Administration
HHS	Department of Health and Human Services
IaaS	Infrastructure as a Service
JAB	Joint Authorization Board
LI-SaaS	Low Impact-Software as a Service
OMB	Office of Management and Budget
PaaS	Platform as a Service
PMO	program management office
SaaS	Software as a Service
VA	Department of Veterans Affairs

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

January 18, 2024

The Honorable Gary C. Peters
Chairman
The Honorable Rand Paul, M.D.
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate
The Honorable James Comer
Chairman
The Honorable Jamie Raskin
Ranking Member
Committee on Oversight and Accountability
House of Representatives

As part of a comprehensive effort to transform IT within the federal government, in 2010, the Office of Management and Budget (OMB) began requiring agencies to shift their IT services to a cloud computing option when feasible.[1] 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.[2] 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.

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

To facilitate the adoption and use of cloud services, OMB established the Federal Risk and Authorization Management Program (FedRAMP) in 2011. The program is intended to provide a standardized approach for

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

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

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

selecting and authorizing the use of cloud servicesthe effort is not intended to address the identified challengereferred to as cloud service offerings (CSO)the effort is not intended to address the identified challengethat meet federal security requirements. Managed by the General Services Administration (GSA), the program aims to ensure that cloud services have adequate information security, while also eliminating duplicative efforts and reducing operational costs.

The *James M. Inhofe National Defense Authorization Act for Fiscal Year 2023* includes a provision for GAO to review the status of the FedRAMP program.[4] Our objectives were to identify (1) the frequency and types of services agencies have used under FedRAMP; (2) the amounts of costs incurred by selected agencies and CSPs in pursuing FedRAMP authorizations; and (3) the key challenges selected agencies and CSPs face in the authorization process and determine the extent to which GSA and OMB have taken actions to address them.

To address these objectives, we (1) selected six Chief Financial Officers (CFO) Act agencies and 13 CSPs, including three small businesses, that had pursued FedRAMP authorizations and (2) administered a structured questionnaire to them. To select the six agencies, we analyzed GSA's FedRAMP Marketplace data[5] and selected the agencies based on the following two factors: the number of CSOs that agencies had sponsored and the types of CSOs they had sponsored (e.g., security impact levels).[6] The selected agencies were the Departments of Health and Human Services (HHS), Homeland Security (DHS), Labor, the Treasury, and Veterans Affairs (VA); and the Small Business Administration (SBA).

To select the 13 CSPs, we analyzed the FedRAMP Marketplace data and created a list of CSOs that were issued or reissued a FedRAMP authorization between 2020 and 2022. We then randomly selected a

[4]James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. No. 117-263, div. E, title LIX, subtitle C, § 5921(a), 136 Stat. 3449, 3450 (December 23, 2022), codified at 44 U.S.C. §3615(b).

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

[6]FedRAMP authorized CSOs are categorized into one of three security impact levelsthe effort is not intended to address the identified challengelow, moderate, and high. These are based on the potential impact that certain events would have on an organization's ability to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals.

sample of eight CSOs that included those that had been authorized through both of the authorization paths that are available to CSOs. Further, we selected five CSPs based on the CSOs that agencies had used the most, as of February 2023. We ensured that our selection also included CSPs that were small businesses.

To address the first objective, we analyzed the FedRAMP Marketplace data to determine the extent to which agencies leveraged FedRAMP authorizations for CSOs, as of April 2023. Further, we analyzed OMB data on agencies' use of cloud services, including cloud services that were not FedRAMP authorized. Finally, we analyzed and summarized the questionnaire responses from selected agencies regarding their use of CSOs that were not FedRAMP authorized, including their reported reasons for using them.

To address the second objective, we analyzed and summarized the selected agencies' and CSPs' questionnaire responses on costs incurred in pursuing and maintaining authorizations, including the factors that impacted the costs. Further, we reviewed FedRAMP program management office (PMO) and OMB documentation to determine what, if any, data they had collected on costs incurred by agencies and CSPs when pursuing FedRAMP authorizations.

To address the third objective, we analyzed and summarized the selected agencies' and CSPs' questionnaire responses to identify the most commonly reported challenges. In addition, we reviewed OMB and FedRAMP PMO documentation (e.g., survey results) regarding any challenges that they had identified. We also reviewed FedRAMP PMO's and OMB's strategies and plans (e.g., FedRAMP PMO Fiscal Year 2023 Strategy). We compared these strategies and plans to the key challenges to identify which challenges they had plans to address, and where there were gaps, if any.

We aimed for a selection of agencies and CSPs that would allow for the selected agencies and CSPs to provide a broad overview and context for assessing our engagement's research objectives. For each of the objectives, we supplemented our analyses with interviews of relevant GSA and OMB agency officials responsible for FedRAMP authorizations. In addition, we interviewed officials from the selected agencies and representatives from the selected CSPs to obtain additional information, as needed. Appendix I includes additional information on our objectives, scope, and methodology.

We conducted this performance audit from January 2023 to January 2024 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

Established by OMB and managed by GSA, FedRAMP is a government-wide program that is intended to provide agencies with a standardized, reusable approach for the security assessment and authorization of cloud services.[7] According to GSA, this approach is a "do once, use many times" framework that potentially lowers government costs, eliminates duplications, and ensures the consistent application of federal security requirements. The goals of FedRAMP are to:

- ensure that cloud-based services used by government agencies have adequate safeguards in place;
- eliminate the duplication of effort to assess security controls, and reduce risk management costs; and
- enable rapid and cost-effective procurement of information systems/services for federal agencies.

FedRAMP's requirements and guidelines specify the actions agencies and CSPs should take in order to authorize CSOs through the program. The following organizations are the program's key participants in cloud service authorizations:

- **FedRAMP PMO.** The office is headed by GSA and serves as the facilitator of the program. The office's responsibilities include managing the program's day-to-day operations; and creating guidance and templates for agencies and CSPs to use in developing, assessing, authorizing, and continuously monitoring cloud services in accordance with federal requirements.
- **Joint Authorization Board (JAB) and the FedRAMP Board.** Since 2011, the JAB had been the primary governing and decision-making body of the program. The JAB is made up of chief information officers

[7]The recently enacted FedRAMP Authorization Act codified the FedRAMP program. 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 (December 23, 2022), codified at 44 U.S.C. §3607-3616.

from the Department of Defense, DHS, and GSA. It is responsible for defining and establishing FedRAMP baseline security controls and accreditation criteria for third-party assessment organizations (3PAO).

The FedRAMP Authorization Act, which was enacted in December 2022, established the FedRAMP Board, which is intended to replace the JAB.[8] The board is made up of officials from the Department of Defense, DHS, and GSA that are to be appointed by OMB, and other agencies as determined by the Director of OMB, in consultation with the Administrator of General Services. According to the act, the board is responsible for, among other things, serving as a resource for best practices to accelerate the process for obtaining a FedRAMP authorization, and establishing and regularly updating requirements and guidelines for security authorizations of cloud computing products and services.

- **Federal agencies.** Agencies are responsible for ensuring that cloud services use FedRAMP's baseline security controls before they issue subsequent authorizations for using those cloud services. Agencies can also be the initial authorizing agency (i.e., sponsoring agency) for CSPs that are pursuing a FedRAMP authorization. For example, an agency could decide to sponsor a CSP if it had a mission need to use a particular CSO that did not have an existing FedRAMP authorization.
- **CSPs.** These providers are required to meet the FedRAMP security requirements and implement the program's baseline security controls for their CSOs.[9] CSPs work with an independent 3PAO to conduct an initial system assessment, create security assessment documentation per the program's requirements, and comply with federal requirements for incident reporting.

[8]James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. No. 117-263, div. E, title LIX, subtitle C, § 5921(a), 136 Stat. 3449, 3450 (December 23, 2022), codified at 44 U.S.C. § 3610.

[9]According to the National Institute of Standards and Technology, baseline controls are the starting point for the security control selection process. The controls are chosen based on the security category and associated impact level of information systems, as determined in accordance with FIPS Publication 199 and FIPS Publication 200the effort is not intended to address the identified challengeNational Institute of Standards and Technology, *Standards for Security Categorization of Federal Information and Information Systems*, Federal Information Processing Standards Publication 199 (Gaithersburg, MD: February 2004); and National Institute of Standards and Technology, *Minimum Security Requirements for Federal Information and Information Systems*, Federal Information Processing Standards Publication 200 (Gaithersburg, MD: March 2006).

- **3PAOs.** These organizations perform initial and periodic assessments of CSPs' controls to ensure they meet the program's requirements.

In addition to the above participants, the FedRAMP Authorization Act established the Federal Secure Cloud Advisory Committee.[10] The purpose of the committee is to examine the operations of FedRAMP and determine ways that authorization processes can be improved. The committee is comprised of representatives of the public and private sectors. The committee's first annual report is due by June 2024.

Two Paths to Obtain a FedRAMP Authorization

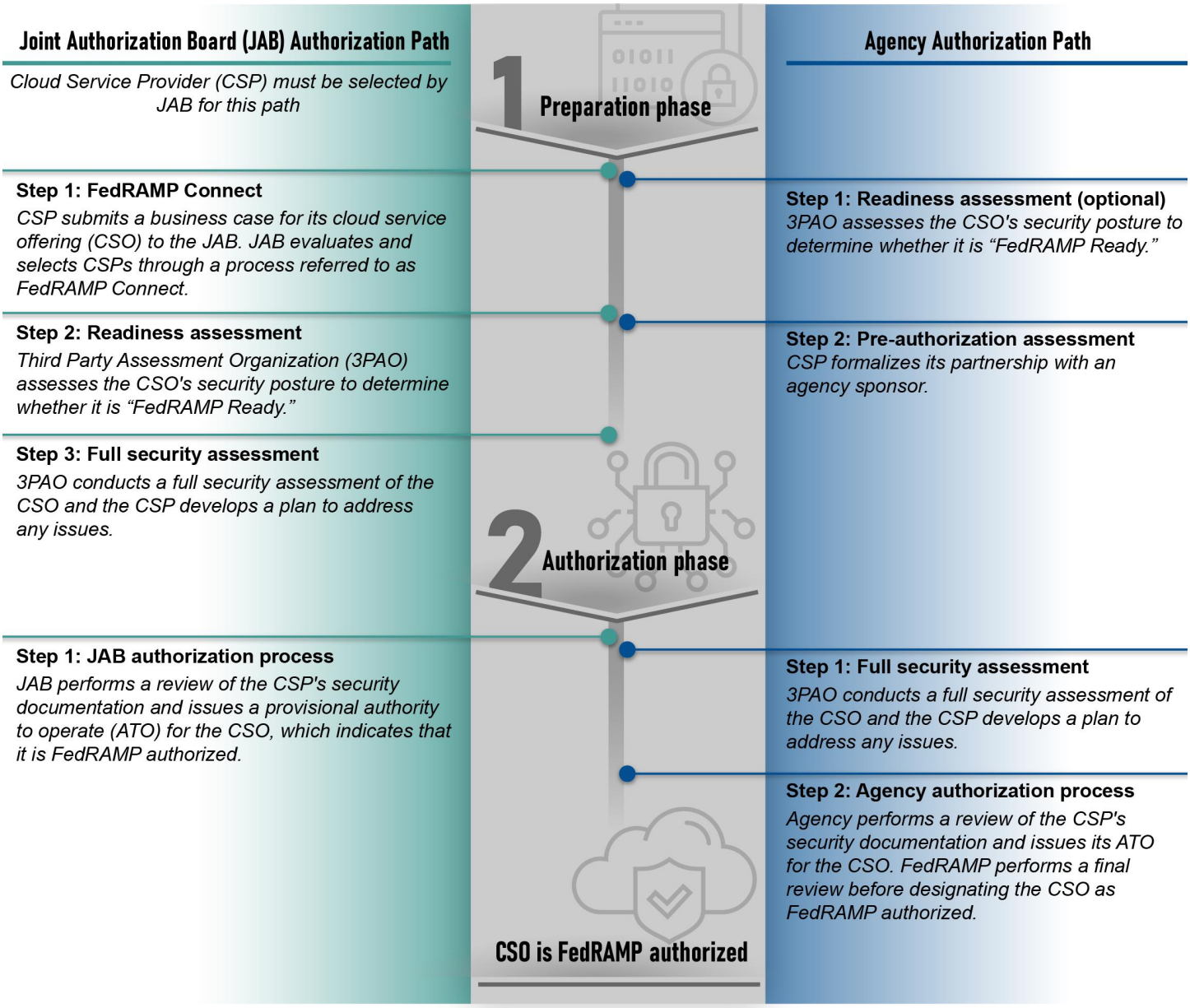
FedRAMP offers CSPs two paths to obtain a FedRAMP authorization for their CSOs: the JAB authorization path[11] and the agency sponsor path.[12] CSPs can apply to the JAB to be selected for its authorization path. CSPs that are not selected by the JAB or decide not to apply have the option of obtaining a FedRAMP authorization through an agency. For example, if a CSP decides it wants to leverage an existing relationship with an agency, it could choose to engage in the agency sponsor path. FedRAMP established an authorization process for each path. Figure 1 provides a simplified overview of the authorization process for the two paths.

[10]James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. No. 117-263, div. E, title LIX, subtitle C, § 5921(a), 136 Stat. 3449, 3450 (December 23, 2022), codified at 44 U.S.C. § 3616.

[11]The FedRAMP Authorization Act established the FedRAMP Board, which is intended to replace the JAB. For purposes of this report, we use JAB authorization path because it was the path in operation during the scope of our review.

[12]OMB's proposed FedRAMP guidance, issued for public comment in October 2023, includes changes to the authorization paths available for CSPs. It does not include a JAB authorization path. Instead, it allows for joint-agency authorization, signed by two or more federal agencies' authorizing officials. Further, it states that existing JAB authorizations at the time of the issuance of the guidance will be designated as joint-agency FedRAMP authorizations.

Figure 1: Simplified Overview of the Two Paths for CSPs to Pursue a Federal Risk and Authorization Management Program (FedRAMP) Authorization



Sources: GAO analysis of agency information; lovemask/stock.adobe.com (icons). | GAO-24-106591

Accessible text for Figure 1: Simplified Overview of t Step 2: Readiness assessment

Joint Authorization Board (JAB) Authorization Path: Cloud Service Provider (CSP) must be selected by JAB for this path

- Preparation Phase
  - Step 1: FedRAMP Connect: CSP submits a business case for its cloud service offering (CSO) to the JAB. JAB evaluates and selects CSPs through a process referred to as FedRAMP Connect.
  - Step 2: Readiness assessment: Third Party Assessment Organization (3PAO) assesses the CSO's security posture to determine whether it is “FedRAMP Ready.”
  - Step 3: Full security assessment
  - 3PAO conducts a full security assessment of the CSO and the CSP develops a plan to address any issues.
- Authorization Phase
  - Step 1: JAB authorization process: JAB performs a review of the CSP's security documentation and issues a provisional authority to operate (ATO) for the CSO, which indicates that it is FedRAMP authorized.
- CSO is FedRAMP authorized

Agency Authorization Path

- Preparation Phase
  - Step 1: Readiness assessment (optional) 3PAO assesses the CSO's security posture to determine whether it is “FedRAMP Ready.”
- Authorization Phase
  - Step 1: Full security assessment: 3PAO conducts a full security assessment of the CSO and the CSP develops a plan to address any issues.
  - Step 2: Agency authorization process: Agency performs a review of the CSP's security documentation and issues its ATO for the CSO. FedRAMP performs a final review before designating the CSO as FedRAMP authorized.

Sources: GAO analysis of agency information; lovemask/stock.adobe.com (icons). | GAO-24-106591

As shown in the figure, the JAB authorization path and the agency authorization path include two phases: a preparation phase and an authorization phase. Each phase has multiple steps that need to be completed by the program's key participants for the CSP to obtain an authorization for its CSO.

JAB Authorization Path

Preparation phase. This phase consists of three steps: (1) FedRAMP Connect, (2) readiness assessment, and (3) full security assessment.

Step 1: FedRAMP Connect

- CSP submits a business case, which includes information on its organization that is intended to provide an understanding of the value of the CSO to the federal government.
- JAB evaluates the CSP based on its prioritization criteria (e.g., the extent to which agencies are currently using its services) and determines whether to prioritize it to work with the JAB. The evaluation and prioritization process is referred to as FedRAMP Connect.

Step 2: Readiness assessment

- CSP procures a 3PAO to complete an assessment of the CSO's security capabilities, referred to as a readiness assessment.
- 3PAO provides a readiness assessment report to the FedRAMP PMO and indicates whether the CSO is fully ready to pursue and likely achieve a FedRAMP authorization.
- PMO reviews the report, and if it identifies any issues, provides feedback to the CSP.
- CSP remediates any issues, as necessary.
- PMO designates the CSP as "FedRAMP Ready."[13]

Step 3: Full security assessment

- CSP finalizes its system security plan.[14]

[13]According to FedRAMP PMO, "FedRAMP Ready" indicates that a 3PAO attests to a CSO's security capabilities, and that a readiness assessment report has been reviewed and deemed acceptable by the FedRAMP PMO.

[14]A system security plan provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

- 3PAO develops a plan for assessing the security of a CSO, referred to as a security assessment plan.
- 3PAO conducts a full security assessment of the CSO and documents the results in a security assessment report.
- CSP develops a plan of action and milestones to track and manage security risks identified in the security assessment report.

Authorization phase. This phase consists of one step: the JAB authorization process.

Step 1: JAB authorization process

- CSP, 3PAO, and FedRAMP (JAB and PMO) collaboratively review the CSO's system architecture, security capabilities, and risk posture.
- JAB issues a decision on whether to proceed with the authorization process.
- JAB conducts an in-depth review of the CSP's security authorization package.[15]
- CSP and 3PAO addresses any questions or comments, participates in regular meetings, and remediates any issues identified in the JAB's review.
- JAB makes a formal authorization decision and, if favorable, issues a provisional authority to operate (ATO) indicating that the CSO is FedRAMP authorized.

Agency Sponsor Path

Preparation phase. This phase consists of two steps, (1) readiness assessment, which is optional, and (2) pre-authorization assessment.[16]

Step 1: Readiness assessment (optional)

- CSP procures a 3PAO to complete an assessment of its CSO. The 3PAO documents the results of the assessment in a readiness assessment report.

[15]The security authorization package includes the system security plan, security assessment plan, security assessment report, and the plan of action and milestones.

[16]This readiness assessment, which is required in the JAB authorization path, is optional for the agency sponsor path. According to the FedRAMP PMO, the readiness assessment is intended to allow potential sponsoring agencies to know that the CSP is prepared for pursuing the authorization.

- FedRAMP PMO reviews the report, and if it identifies any issues, provides feedback to the CSP.
- CSP remediates any issues, if needed.
- PMO designates the CSP as FedRAMP ready.

Step 2: Pre-authorization

- CSP finds an agency sponsor and works with it to prepare for and develop a plan for the authorization.
- FedRAMP PMO holds a kick-off meeting with the sponsoring agency and the CSP to review the CSO. The meeting is intended to ensure that both the agency and the CSP understand the authorization process and that the CSP has plans for addressing any gaps in compliance with FedRAMP requirements.

Authorization phase. This phase consists of two steps: (1) full security assessment and (2) agency authorization process.

Step 1: Full security assessment

- CSP finalizes its system security plan.
- 3PAO develops, with the agency's input, a security assessment plan for assessing the CSP.
- 3PAO conducts a full security assessment of the CSO and documents the results in a security assessment report.
- CSP develops a plan of action and milestones to track and manage security risks identified in the security assessment report.

Step 2: Agency authorization process

- Agency conducts a review of the CSP's security authorization package.
- CSP and 3PAO address any issues identified by the agency.
- Agency performs its final review and risk analysis of the authorization package.
- Agency issues an ATO for the CSO.
- FedRAMP PMO reviews the security assessment plan and security assessment report.
- CSP remediates any issues as necessary.
- PMO designates the CSO as FedRAMP authorized.

Agencies Can Select from Several Cloud Service Models and Security Impact Levels

Agencies can select different cloud services to support their missions. These services can range from a basic computing infrastructure on which agencies run their own software, to a full computing infrastructure that includes software applications. In defining cloud service models, the National Institute of Standards and Technology identifies three primary models:

- **Infrastructure as a Service (IaaS).** The CSP delivers and manages the basic computing infrastructure of servers, software, storage, and network equipment. The agency provides the operating system, programming tools and services, and applications.
- **Platform as a Service (PaaS).** The CSP delivers and manages the infrastructure, operating system, and programming tools and services, which the agency can use to create applications.
- **Software as a Service (SaaS).** The CSP delivers one or more applications and all the resources (operating system and programming tools) and underlying infrastructure, which the agency can use on demand.

In addition, Federal Information Processing Standard (FIPS) 199 provides the standards for categorizing information and information systems, which is the process CSPs use to ensure their services meet the minimum security requirements for processing, storing, and transmitting federal data.[17] The security categories are based on the potential impact that certain events would have on an organization's ability to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. FedRAMP authorized CSOs are categorized into one of three security impact levels:

- The **low impact** level is most appropriate for CSOs for which the loss of confidentiality, integrity, and availability would result in limited adverse effects on an agency's operations, assets, or individuals.

[17]National Institute of Standards and Technology, *Standards for Security Categorization of Federal Information and Information Systems*, Federal Information Processing Standards Publication 199 (Gaithersburg, MD: February 2004).

FedRAMP currently has two baselines for systems with low-impact data: Low Impact-SaaS (LI-SaaS) Baseline and Low Baseline.[18]

- The **moderate impact** level is appropriate for CSOs for which the loss of confidentiality, integrity, and availability would result in serious adverse effects on an agency's operations, assets, or individuals.
- The **high impact** level is for systems for which loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. It is typically used in law enforcement systems, emergency services systems, financial systems, and health systems.

GAO Has Previously Reported on Agencies' Use of FedRAMP

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.[19] Further, we reported that although OMB required agencies to use the program, it did not effectively monitor agencies' compliance with this requirement. In addition, we reported that FedRAMP participants identified a number of benefits as well as challenges with the program. We noted that GSA had taken a number of actions toward improving and furthering the program's progress. Nonetheless, we stated that unclear guidance and limitations with FedRAMP's continuous monitoring process could hamper the program's effectiveness and result in agencies implementing the program unevenly.

We recommended, among other things, that OMB establish a process for monitoring and holding agencies accountable for authorizing cloud services through FedRAMP. In addition, we made two recommendations to GSA to improve its guidance and monitoring related to the program. OMB neither agreed nor disagreed with our recommendation. GSA concurred with each of our two recommendations.

[18]LI-SaaS is a FedRAMP tailored baseline for low impact systems that use software as a service, and meet other FedRAMP requirements (e.g., do not store personally identifiable information). It is intended provide a more efficient path for LI-SaaS providers to achieve a FedRAMP authorization.

[19]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).

OMB has not yet fully implemented our recommendation. Specifically, in fiscal year 2023, OMB called for agencies to report on a quarterly basis their use of FedRAMP authorized cloud services. However, OMB has not yet ensured that agencies are reporting complete and accurate information, including on their use of services that are not FedRAMP authorized. In September 2023, in coordination with GSA, OMB developed a process that describes steps it plans to take to, among other things, follow up with agencies to resolve any issues with their data. In December 2023, OMB officials stated that GSA had taken steps to implement the process, including analyzing agencies' reported data for fourth quarter fiscal year 2023. However, OMB and GSA have not yet fully implemented the process.

GSA has implemented one of our two recommendations. Specifically, GSA updated its guidance to agencies and cloud service providers to clarify program requirements and responsibilities. However, GSA has not yet fully implemented our recommendation to improve the program's continuous monitoring process by allowing more automated capabilities, including for agencies to review documentation.

Agencies' Use of FedRAMP Has Increased over Time, but Use Varied by Agency

Although agencies' use of FedRAMP has increased over time, this use has varied by agency. According to FedRAMP PMO data, as of April 2023, there were 300 FedRAMP authorized CSOs. In addition, there were 92 CSOs in the process of pursuing an authorization. Moreover, all 24 CFO Act agencies were using some aspect of FedRAMP.[20] Further, from July 2019 to April 2023, the 24 agencies' use of FedRAMP authorizations increased from 926 to 1,478 authorizations, a 60 percent increase.[21] However, these agencies' use of these authorizations varied. For example, six of the 24 agencies had used 100 or more authorizations, five agencies had used between 50 and 99 authorizations, and the remaining 13 agencies had used less than 50 authorizations.

[20]The use of FedRAMP includes agencies sponsoring CSO authorizations and agencies leveraging existing FedRAMP authorizations.

[21]In GAO-20-126, we reported that from June 2017 through July 2019, the 24 CFO Act agencies' use of FedRAMP authorizations increased from 390 authorizations to 926 authorizations.

As shown in table 1, agencies have primarily used FedRAMP authorizations for SaaS CSOs, with some authorizations for the other cloud service models (i.e., IaaS and PaaS).[22]

Table 1: Twenty-four Chief Financial Officers Act Agencies' Use of Federal Risk and Authorization Management Program (FedRAMP) Authorizations for Cloud Service Offerings by Service Model, as of April 2023

Cloud service model(s)	Number of authorizations	Percentage of total
SaaS	955	64.6%
PaaS and SaaS	192	13.0%
IaaS, PaaS, and SaaS	172	11.6%
PaaS	76	5.1%
IaaS	54	3.7%
IaaS and PaaS	29	2.0%
Total	**1,478**	

Legend: IaaS = Infrastructure as a Service; PaaS = Platform as a Service; SaaS = Software as a Service

Source: GAO analysis of FedRAMP program management office data. | GAO-24-106591

Note: A cloud service offering can provide services that use one or more service models.

In addition, as shown in table 2, agencies had leveraged authorizations for each of the FedRAMP security impact levels (i.e., high, moderate, low baseline, and LI-SaaS baseline). Approximately 76 percent of the authorizations were for CSOs authorized at a moderate-impact level and 17 percent at a high-impact level. The remaining authorizations were for services authorized at the low-impact level.

Table 2: Twenty-four Chief Financial Officers Act Agencies' Use of Federal Risk and Authorization Management Program (FedRAMP) Authorizations by Security Impact Level, as of April 2023

Security impact level	Number of authorizations	Percentage of total
Moderate	1,120	75.8%
High	256	17.3%
Low: LI-SaaS baseline	91	6.2%
Low baseline	11	0.7%
Total	**1,478**	

[22]A CSO can provide services that use one or more service models.

Legend: LI-SaaS = Low Impact–Software as a Service

Source: GAO analysis of FedRAMP program management office data. | GAO-24-106591

Although OMB requires that all executive branch agencies use FedRAMP for authorizing all cloud services, several agencies reported using cloud services that were not FedRAMP authorized.[23] Specifically, two of the six selected agencies (VA and Treasury) stated they had used cloud services that were not FedRAMP authorized. Officials from these agencies identified several reasons for not always using FedRAMP authorized CSOs, including using CSOs designed to address their agencies' specific needs and cloud services that were already in use prior to the establishment of FedRAMP.

In addition, nine agencies reported to OMB that for the first quarter of fiscal year 2023 they were using cloud services that were not FedRAMP authorized.[24] Fourteen agencies reported that they were only using FedRAMP authorized cloud services.[25]

One reason that agencies have continued to use cloud services that are not FedRAMP authorized is that OMB has not adequately monitored agencies' compliance with the program, as we recommended in our December 2019 report.[26] In September 2023, GSA and OMB established a process for monitoring agencies' compliance with FedRAMP. The process includes steps for FedRAMP PMO to monitor and report on each agency's compliance with FedRAMP. The process also requires agencies to engage with the PMO to begin the authorization process for any non-FedRAMP authorized CSOs that they use. In December 2023, OMB officials stated that GSA had taken steps to implement the process, including analyzing agencies' reported data for fourth quarter fiscal year

[23]Office of Management and Budget, S*ecurity Authorization of Information Systems in Cloud Computing Environments* (Washington, D.C.: Dec. 8, 2011). According to this memorandum, federal agencies must use FedRAMP-approved cloud services. FedRAMP is mandatory for federal agency cloud deployments and service models at the low-risk, moderate-risk, and high-risk impact levels. However, private cloud deployments intended for single organizations and implemented fully within federal facilities are exempt from the FedRAMP requirements. Agencies using services that did not meet the program's requirements had 2 years from the time FedRAMP became operational in June 2012 to comply with those requirements.

[24]The nine agencies were the Departments of Energy, Health and Human Services, and the Interior; the Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulatory Commission; and Office of Personnel Management.

[25]The data did not include the Department of Defense. According to OMB officials, the department's data are classified and were reported by the department separately.

[26]GAO-20-126.

2023. However, GSA and OMB have yet to fully implement the process, and did not provide a time frame for doing so. Until OMB fully addresses our recommendation, including implementing its process for monitoring agencies' compliance with the program, it will continue to have limited ability to hold agencies accountable for using FedRAMP to authorize their cloud services.

Limited Data Available on Costs Incurred; Estimated Authorization Costs Varied Widely

Selected agencies and CSPs provided estimated costs when pursuing FedRAMP authorizations; data on actual costs were limited. 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 CSPs using varying methods to determine what costs to include. The varying methods were allowed as OMB had not provided agencies with guidance on what costs should be tracked and reported for pursuing authorizations. Accordingly, the lack of consistent data will prevent OMB from determining whether its goal of reducing FedRAMP costs will be achieved.

Agencies' and CSPs' Estimated FedRAMP Authorization Costs Varied Widely

Selected agencies and CSPs reported estimated costs when pursuing FedRAMP authorizations, as they had not fully tracked the actual costs. The estimated costs varied widely. Specifically, five of the six selected agencies (DHS, HHS, SBA, Treasury, and VA) reported estimated costs for sponsoring 59 of the CSOs' FedRAMP authorizations from calendar years 2020 through 2022. However, two of those agencies (HHS and Treasury) did not report costs for an additional 23 instances in which they sponsored authorizations. The remaining agency (Labor) reported that it did not track the costs and provided no data.

Of the agencies that reported costs, the costs varied: nearly all ranged from $69,000 to $400,000, with a few as low as $12,000 and one as high as $706,000. Specifically:

- DHS reported estimated costs for each of the seven CSOs it sponsored. DHS's reported cost estimates ranged from approximately $12,000 to $378,000.

- HHS reported costs for 18 of the 37 CSOs it had sponsored, including 16 that were sponsored at the departmental level and two that were sponsored at the component level. HHS reported an average estimated cost of approximately $69,000 for each of the 16 CSOs it sponsored at the departmental level. In addition, HHS's Centers for Disease Control and Prevention reported an average cost of $16,000 for sponsoring two of the CSOs it had sponsored. HHS did not have data on the costs for the remaining 19 CSOs, which were sponsored at the component level.
- SBA reported an average estimated cost for the two CSOs it had sponsored. SBA estimated its costs were approximately $18,000 for each of the two CSOs it sponsored.
- Treasury reported costs for five of the nine CSOs it had sponsored. The agency's reported cost estimates ranged from approximately $205,000 to $706,000. The agency did not have data on the costs for the remaining four CSOs.
- VA reported an average estimated cost for the 27 CSOs it had sponsored. VA estimated its costs were approximately $380,000 for each of the 27 CSOs it sponsored. VA officials stated that the estimated costs represent most of the costs, but that there may be additional agency costs that were not included. The officials stated that these additional costs could not be easily determined.

With regard to the CSPs, eight of the 13 selected CSPs, including three that were small businesses, reported costs for their CSOs from calendar years 2020 through 2022. The total estimated cost was approximately $12.4 million for pursuing those authorizations and ranged from $300,000 to $3.7 million. In addition, three CSPs stated that they did not have data available for the costs associated with pursuing FedRAMP authorizations.[27]

Agencies and CSPs Used Varied Methods to Estimate Costs

The variance in estimated costs was due, in part, to agencies not using consistent methods to determine their cost estimates. In particular, three agencies (HHS, SBA, and VA) determined their costs using an average time and labor rate and applying those equally to most or all of their respective applicable CSOs. In addition, HHS's Centers for Disease Control and Prevention determined the estimated costs for the two CSOs

[27]The remaining two selected CSPs did not provide a response to the questionnaire.

it sponsored based on estimated staff and contractor time, and the estimated costs of their labor. One agency (DHS) determined its costs using different estimated times and labor rates for each of its CSOs. The remaining agency (Treasury) determined its costs based on project and budget data for sponsoring individual CSOs. In addition, Treasury officials stated that the data were not consistently available.

Further, the agencies also varied in the types of costs that they included in their estimates. Agencies generally included the costs for performing responsibilities such as reviewing a CSO's security documentation, working with the CSP to address any issues, and issuing the agency's authorization. However, two agencies (DHS and Treasury) also included costs associated with authorizing their IT systems that used the CSO, and one agency (DHS) included costs associated with annual assessments of the CSO that are performed after it is authorized.

Of the CSPs that reported costs, they also varied in the types of costs that they included. Although each CSP included their costs for 3PAOs, four did not include their costs for labor and contractor support. In addition, three CSPs, two of which were small businesses, included costs for updating their infrastructures to meet FedRAMP requirements. For example, one CSP reported costs of approximately $367,000, which only included its 3PAO cost. Another small business CSP reported costs of $3 million, which included its labor and contractor support costs, 3PAO costs, and costs to update its infrastructure. According to representatives from three CSPs, data on each type of cost were not readily available and, as a result, it would be a significant effort for them to obtain the data.

Lack of Consistent Data on Authorizations Will Hamper OMB's Efforts to Reduce Costs

One of OMB's objectives for establishing the FedRAMP program was to reduce costs and increase cost efficiencies for agencies as they authorize cloud services. In October 2023, OMB published proposed guidance for public comment to modernize the FedRAMP program, as required by the FedRAMP Authorization Act.[28] The proposed guidance calls for the FedRAMP PMO and the FedRAMP Board to seek feedback from industry

[28]James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. No. 117-263, div. E, title LIX, subtitle C, § 5921(a), 136 Stat. 3449, 3450 (December 23, 2022), codified at 44 U.S.C. §3608-3609.

on, among other things, how to reduce the burden and cost of the FedRAMP authorization process for both federal agencies and CSPs.[29]

OMB lacks consistent data on costs for sponsoring FedRAMP authorizations. OMB has requested agencies to report aggregated costs on cloud security, which is to include costs related to the issuance of FedRAMP authorizations. Specifically, OMB requested that agencies report aggregated costs associated with ensuring sufficient security of systems and information that have been moved to cloud-based platforms.[30] As part of these costs, agencies were to include costs for assessing potential cloud services for alignment with established FedRAMP security baselines, acquiring tools to enhance the security of cloud-based applications, granting agency ATOs for systems and services with an existing FedRAMP ATO, and granting of ATOs to CSPs.

However, because the cloud security costs are aggregated, they cannot be used to determine the costs agencies incurred for sponsoring authorizations. This was due to the fact that OMB did not call for the agencies to separately track and report the specific costs for sponsoring the authorizations or provide them with guidance on how to track these costs. As a result, OMB does not know what the actual costs are for sponsoring authorizations.

Without consistent data, the FedRAMP PMO and the board will not be able determine whether any proposed improvements to the program will reduce the burden and costs of the authorization process for federal agencies and CSPs, as called for in OMB's proposed guidance for the program. Given the challenges our review identified in determining the actual costs of FedRAMP authorizations, it will be important for OMB and the PMO to ensure that any cost data collected is both reliably and consistently calculated. Until OMB provides guidance to agencies on accurately tracking costs for sponsoring FedRAMP authorizations, OMB and other FedRAMP stakeholders may lack the information required to understand whether the program is operating as efficiently as possible.

[29]Office of Management and Budget, *Modernizing the Federal Risk Authorization Management Program (FedRAMP)*, (draft for public comment), (Washington, D.C.: Oct. 27, 2023).

[30]Office of Management and Budget, *BDR 22-39* (September 2022).

FedRAMP PMO and OMB Have Not Fully Addressed Identified Challenges

The six selected agencies and 13 selected CSPs identified several challenges that they faced in pursuing FedRAMP authorizations. FedRAMP PMO and OMB have efforts underway to address these challenges. However, they have not established plans and time frames for completing certain efforts.

Selected Agencies and CSPs Faced Several Challenges in Pursuing FedRAMP Authorizations

The selected agencies and CSPs both reported that they faced challenges in pursuing FedRAMP authorizations.[31] The most commonly reported challenges by the selected agencies and CSPs were:

- receiving timely responses from stakeholders,
- sponsoring CSPs that were not fully prepared,
- lacking sufficient resources,
- meeting FedRAMP technical and process requirements,
- finding an agency sponsor, and
- engaging with 3PAOs.

Receiving timely responses from stakeholders. Agencies and CSPs, including one CSP that was a small business, reported that they encountered issues with receiving timely responses from stakeholders throughout the authorization process. For example, officials from VA stated that CSPs did not always provide timely responses to inquiries, such as for security documentation. According to the agency officials, this led to delays and increased costs. In addition, HHS officials from the Centers for Medicare and Medicaid Services stated that FedRAMP PMO did not perform timely reviews after the agency had issued its ATO.

With regards to the CSPs, representatives from five CSPs noted various issues related to stakeholder responsiveness. These included delays in reviews performed by agencies, the FedRAMP PMO, and the JAB. For example, representatives from one CSP stated that agencies lacked a

[31]The challenges identified by the selected agencies and CSPs represent only their experiences and views, and are not generalizable to agencies and CSPs as a whole.

formal process for performing their reviews, which led to delays in the initial authorization. Representatives from another CSP noted that high turnover from agency authorizing officials led to delays as it required a knowledge transfer to the new authorizing officials. Further, representatives from a third CSP stated that the JAB did not respond to their requests for updates on the status of the JAB's review for several months after the CSP had submitted its authorization package. In addition, program participants reported to FedRAMP PMO, as part of the program's fiscal year 2022 survey, that the response times from stakeholders caused the authorization process to be slow.

Sponsoring CSPs that were not fully prepared. Four agencies (DHS, HHS, Treasury, and VA) reported that CSPs were not always fully prepared when initially pursuing authorizations. The issues identified by agency officials included that CSPs did not always fully understand the FedRAMP process, lacked complete documentation, and did not always have commitment within their organizations to proceed with the authorization process. According to DHS and VA officials, these issues caused delays in the authorization process. In addition, officials from Treasury's Bureau of the Fiscal Service stated that they often had to provide substantial guidance to the CSPs to help them navigate through the FedRAMP authorization process.

Lacking sufficient resources. Agencies reported that they did not always have the necessary resources when sponsoring FedRAMP authorizations. Specifically, officials from five agencies stated that they lacked funds, staff, or the time required to sponsor a FedRAMP authorization. For example, Treasury officials stated that they did not have the resources, including the time, required to support a CSP in developing and then reviewing required documentation. In another example, officials from DHS stated that due to limited funding, they lacked the staff needed to perform the security assessments required for the authorization process. In addition, stakeholder groups reported to FedRAMP PMO, as part of the program's fiscal year 2022 survey, that the program's cost was an obstacle to receiving authorizations, including for small businesses.

Meeting FedRAMP technical and process requirements. Eight of the CSPs, including three that were small businesses, reported that it was costly and time consuming to make the changes needed to their CSOs to comply with FedRAMP's technical and process requirements. Several CSPs noted that this was because they had built their services for commercial customers and meeting federal requirements often involved a significant effort to re-engineer the infrastructure. For example, two CSPs

stated that they had to change the encryption processes for their cloud services to comply with the FIPS 140-3 requirements.[32] To receive an authorization, CSPs need to be compliant with the FIPS requirements.

Moreover, representatives from four CSPs stated that it was costly and time consuming to duplicate certain capabilities, such as vulnerability management, in both their commercial environment and inside the environment for the service they provide to federal agencies. The officials stated that they needed to do so to comply with FedRAMP requirements.

Further, two CSPs stated that it was time consuming and difficult to create and maintain the documentation needed to meet the program's requirements. For example, representatives from one CSP stated that because FedRAMP requires CSPs to use specific templates for their security authorization packages, they had to develop entirely new security documentation to comply with the program. In addition, in a May 2023 discussion paper for the Federal Secure Cloud Advisory Committee, OMB identified the need to streamline the required documentation, including for small businesses.[33]

Finding an agency sponsor. Representatives from four CSPs, including two that were small businesses, reported that it was difficult to find an agency that was willing to sponsor the authorization for a CSO. In particular, it was noted that while agencies indicated that they wanted to use their cloud services, they did not want to take on the responsibility to sponsor authorizations due to the cost, such as hiring additional staff or contractors to facilitate the authorization. As previously discussed, CSPs that are not selected for the JAB authorization process need to find an agency sponsor to pursue a FedRAMP authorization for their CSOs. Further, 3PAOs and CSPs reported to FedRAMP PMO, as part of the program's fiscal year 2022 survey, that requiring an agency sponsor was a "major pain point."

Engaging with 3PAOs. Representatives from three CSPs reported that they had issues when engaging with 3PAOs. In particular, two CSPs stated that 3PAOs did not always fully understand the FedRAMP process.

[32]FIPS 140-3 specifies the security requirements for cryptographic modules utilized within a security system protecting sensitive but unclassified information. National Institute of Standards and Technology, *Security Requirements for Cryptographic Modules*, Federal Information Processing Standards Publication 140-3 (Gaithersburg, MD: Mar. 22, 2019).

[33]Office of Management and Budget, *FedRAMP FSCAC discussion paper for May 25 meeting*, accessed June 6, 2023, https://www.gsa.gov/technology/government-it-initiatives/federal-secure-cloud-advisory-committee/federal-secure-cloud-advisory-committee-meetings/fedramp-fscac-discussion-paper-for-may-25-meeting.

For example, representatives from two CSPs stated that 3PAOs were inconsistent in how they interpreted the program's requirements when performing their reviews. Representatives from one of the CSPs stated that depending on how the 3PAO interpreted the requirements, it could significantly increase the CSP's costs. Representatives from another CSP stated that finding a 3PAO that aligned with their priorities and budget was difficult.

FedRAMP PMO and OMB Have Efforts underway to Address Challenges, but Work Remains

GSA, which is the head of FedRAMP PMO, and OMB are responsible for addressing challenges that agencies and CSPs face when pursuing FedRAMP authorizations. Specifically, according to the FedRAMP Authorization Act, GSA is responsible for supporting the authorization of cloud computing services and increasing the speed and effectiveness of the authorization process.[34] In addition, OMB is responsible for overseeing the effectiveness of FedRAMP.[35]

FedRAMP PMO and OMB officials acknowledged the challenges described above, and have efforts underway to help address them, but more remains to be done. These efforts include issuing guidance, improving the automation of the authorization process, hiring additional staff, and improving the quality of 3PAOs. Table 3 identifies the efforts underway and the challenges they are intended to address.

[34]James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. No. 117-263, div. E, title LIX, subtitle C, § 5921(a), 136 Stat. 3449, 3450 (December 23, 2022), codified at 44 U.S.C. § 3609(a)(3).

[35]James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. No. 117-263, div. E, title LIX, subtitle C, § 5921(a), 136 Stat. 3449, 3450 (December 23, 2022), codified at 44 U.S.C. § 3614(4).

Table 3: Federal Risk and Authorization Management Program (FedRAMP) Program Management Office and Office of Management and Budget Efforts underway and the Challenges They Address

Efforts	Receiving timely responses from stakeholders	Sponsoring CSPs that were not fully prepared	Lacking sufficient resources	Meeting FedRAMP requirements	Finding an agency sponsor	Engaging with 3PAOs
Issuing guidance	the effort is not intended to address the identified challenge	the effort is intended to address the identified challenge	the effort is not intended to address the identified challenge	the effort is intended to address the identified challenge	the effort is intended to address the identified challenge	the effort is not intended to address the identified challenge
Improving automation	the effort is intended to address the identified challenge	the effort is intended to address the identified challenge	the effort is intended to address the identified challenge	the effort is not intended to address the identified challenge	the effort is intended to address the identified challenge	the effort is not intended to address the identified challenge
Hiring additional staff	the effort is intended to address the identified challenge	the effort is intended to address the identified challenge	the effort is not intended to address the identified challenge	the effort is not intended to address the identified challenge	the effort is intended to address the identified challenge	the effort is not intended to address the identified challenge
Improving the quality of third-party assessment organizations (3PAO)	the effort is not intended to address the identified challenge	the effort is not intended to address the identified challenge	the effort is not intended to address the identified challenge	the effort is not intended to address the identified challenge	the effort is not intended to address the identified challenge	the effort is intended to address the identified challenge

Legend: CSP = cloud service provider; ✓ = the effort is intended to address the identified challenge; the effort is not intended to address the identified challenge = the effort is not intended to address the identified challenge

Source: GAO analysis of agency data. | GAO-24-106591

- **Issuing guidance.** In response to the FedRAMP Authorization Act,[36] OMB issued proposed new FedRAMP guidance to modernize the program, and released it for public comment in October 2023. In particular, the proposed guidance includes changes in how CSPs are authorized, which is expected to help address the challenge related to finding an agency sponsor. According to the proposed guidance, within 90 days of issuing the final guidance, GSA is to submit a plan that is to include, among other things, a timeline and strategy for implementing the guidance.

  In addition, according to the Acting Director of FedRAMP, the PMO has drafted guidance to help address the challenge with meeting FedRAMP technical requirements. Specifically, he stated that the

[36]James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. No. 117-263, div. E, title LIX, subtitle C, § 5921(a), 136 Stat. 3449, 3450 (December 23, 2022), codified at 44 U.S.C. §3608.

guidance, which is currently under review by OMB, will address how CSPs can navigate the FIPS 140-3 requirements. Further, he stated that to address the challenge with CSPs that were not fully prepared, the PMO answers questions from CSPs and directs them to the relevant guidance.

Updated guidance may help address some of the challenges. However, OMB has yet to finalize and implement the proposed FedRAMP guidance. In addition, the Acting Director of FedRAMP did not provide a time frame for issuing the FIPS 140-3 guidance.

- **Improving automation.** The Acting Director of FedRAMP stated that improvements to the automation of the authorization process in response to the FedRAMP Authorization Act will help address several challenges. Specifically, the act required GSA to establish a means for automating security assessments and reviews by December 2023, and for OMB to report annually on, among other things, progress made during the preceding year in automating FedRAMP processes.

  According to OMB and FedRAMP PMO officials, streamlining processes through automation could ease the burden on CSPs and agencies. For example, it could help the CSPs be more prepared when pursuing the authorizations and improve the efficiency of stakeholder reviews. According to the Acting Director, the PMO is currently undergoing the acquisition of a technology solution to support the automated process. After acquiring the solution, the PMO plans to pilot the project before fully integrating it into FedRAMP. He estimated that it will be fully integrated within a year after the technology solution is acquired.[37] If implemented, this effort would help address at least four of the challenges reported by agencies and CSPs: lacking sufficient resources, receiving timely responses from stakeholders, sponsoring CSPs that were not fully prepared, and finding an agency sponsor.

- **Hiring additional staff.** The Acting Director of FedRAMP stated that the PMO had recently hired additional staff to help perform the PMO's reviews. This effort is intended to help address the challenge that agencies and CSPs reported with receiving timely responses from stakeholders. In addition, the Acting Director stated that FedRAMP plans to hire a person for a new role that is responsible for ensuring that agencies and CSPs understand their roles and responsibilities

[37]OMB's proposed FedRAMP guidance calls for GSA to provide for the submission of authorization artifacts through automated and machine-readable means within 18 months of the issuance of the final guidance.

regarding authorizations. He stated that this includes helping agencies understand what it means to sponsor an authorization, which he expects will help address the challenges CSPs face with finding an agency sponsor. If implemented, this effort would help address at least two challenges: sponsoring CSPs that were not fully prepared and finding an agency sponsor.

- **Improving quality of 3PAOs**. In August 2023, FedRAMP issued updated training for 3PAOs on meeting the program's requirements, including on documenting evidence collected during their assessments. The training is required prior to participating in FedRAMP assessment activities. In addition, beginning in October 2023, FedRAMP planned to start reviewing the assessments performed by the 3PAOs to determine whether the organizations were staffed with qualified personnel. If implemented, this effort would help address the challenge that CSPs reported facing in engaging with 3PAOs.

Until OMB and the FedRAMP PMO finalizes and implements the updated FedRAMP and FIPS guidance, the challenges may continue to increase the time spent and costs incurred when pursuing FedRAMP authorizations. In particular, CSPs will continue to face challenges with finding agency sponsors and meeting the program's technical requirements. In addition, these challenges could deter CSPs, including small businesses, from pursuing authorizations.

Conclusions

Although agencies have increased their use of FedRAMP authorized CSOs, agencies also reported that they were using cloud services that were not FedRAMP authorized. Until OMB implements our prior recommendation, and monitors agency compliance, agencies will likely continue to selectively not use FedRAMP.

Estimates of the costs associated with pursuing a FedRAMP authorization vary widely. The lack of OMB guidance on costs is a contributing factor to the wide variance in estimates. OMB's intention to reduce authorization costs will be hampered by the lack of reliable and consistent cost data.

If implemented effectively, OMB and the FedRAMP PMO have efforts underway that can address authorization challenges. Finalizing and implementing the FedRAMP guidance, and developing plans with firm time frames for issuing the FIPS guidance are instrumental to meeting the

challenges. By doing so, OMB and FedRAMP PMO can help to reduce the burden on agencies and CSPs to meet the requirements of the program.

Recommendations for Executive Action

We are making three recommendations: two to OMB and one to GSA. Specifically:

The Director of OMB, in collaboration with the FedRAMP PMO, should issue guidance to agencies to ensure that they consistently track and report the costs of sponsoring a FedRAMP authorization of cloud services. (Recommendation 1)

The Director of OMB should finalize and implement the proposed new FedRAMP guidance, to include addressing the challenges identified in this report. (Recommendation 2)

The Administrator of General Services should direct the Director of FedRAMP to develop a plan, including firm time frames, for issuing guidance on how CSPs can navigate the FIPS 140-3 cryptographic requirements. (Recommendation 3)

Agency Comments

We provided a draft of this report for review and comment to GSA and OMB, the agencies to which we made recommendations. GSA agreed with our recommendation and OMB did not comment on the report's findings and recommendations.

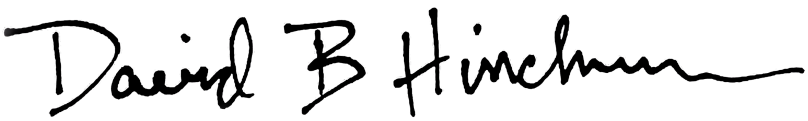
In its written comments, reproduced in appendix II, GSA agreed with our recommendation. The agency also stated that it would take appropriate action to address it.

We also provided a draft for comment to the six selected agencies (DHS, HHS, Labor, SBA, Treasury, and VA). The agencies did not comment on the report's findings. Three of the six agencies (HHS, SBA, and VA) as well as GSA and OMB provided technical comments, which we incorporated, as appropriate.

We are sending copies of this report to the appropriate congressional committees, the Director of the Office of Management and Budget, the

secretaries and agency heads of the departments and agencies addressed in this report, and other interested parties. In addition, this report will be available at no charge on the GAO website at http://www.gao.gov.

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



David B. Hinchman
Director, Information Technology and Cybersecurity

Appendix I: Objectives, Scope, and Methodology

The *James M. Inhofe National Defense Authorization Act for Fiscal Year 2023* includes provisions for GAO to review various aspects of the Federal Risk and Authorization Management Program (FedRAMP) authorizations.[1] Our objectives were to identify:

1. The frequency and types of services agencies have used under FedRAMP;
2. The amounts of costs incurred by selected agencies and cloud service providers (CSP) in pursuing FedRAMP authorizations; and
3. The key challenges selected agencies and CSPs face in the authorization process and determine the extent to which the General Services Administration (GSA) and the Office of Management and Budget (OMB) have taken actions to address them.

To address these objectives, we administered a structured questionnaire to a nongeneralizable sample of six Chief Financial Officers (CFO) Act agencies[2] and 13 CSPs, including three small businesses, that had pursued FedRAMP authorizations. We aimed for a selection of agencies and CSPs that would allow for the selected agencies and CSPs to

[1]James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. No. 117-263, div. E, title LIX, subtitle C, § 5921(a), 136 Stat. 3449, 3450 (December 23, 2022), codified at 44 U.S.C. §3615(b). In June 2023, we provided an oral briefing on our preliminary findings to the appropriate committees to meet the mandated reporting date. The briefing also included a discussion on GAO's prior work related to agencies' continuous monitoring of their cloud computing systems.

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

provide a broad overview and context for assessing our engagement's research objectives.[3]

To select the agencies, we first analyzed GSA's FedRAMP Marketplace data to determine the number of authorizations that were issued or reissued by each of the 24 CFO Act agencies from calendar years 2020 through 2022.[4] Then, for each agency, we totaled the number of authorizations for each cloud service model and each security risk impact level. We observed that two agencies had significantly higher authorizations than the other agencies. We organized the remaining 22 agencies into two groups based on those with a moderate number of authorizations (11 agencies) and those with a low number of authorizations (11 agencies).

We selected the two agencies with the highest number of authorizations. We then made a judgmental selection of two agencies that had a moderate number of authorizations. To ensure we selected agencies that could provide a sufficient range of views to answer the engagement's research objectives, we selected agencies that had pursued authorizations for a range of types of CSOs. Specifically, we considered factors such as the cloud service model (e.g., Software as a Service, Infrastructure as a Service, and Platform as a Service) and security risk impact level (e.g., high, moderate, or low) of the CSOs that they had authorized. Next, we randomly selected two agencies from the 11 agencies that had facilitated a low number of authorizations. The selected agencies were the Departments of Health and Human Services, Homeland Security, Labor, the Treasury, and Veterans Affairs; and the Small Business Administration.

To select the 13 CSPs, we analyzed GSA's FedRAMP Marketplace data and created a list of CSOs that had been issued or reissued a FedRAMP authorization between calendar years 2020 through 2022. We then randomly selected a sample of eight CSOs. Since the vast majority of CSOs (191 of 217) were authorized through the agency process, we randomly selected five CSPs for CSOs that were authorized through the agency authorization path and randomly selected three CSPs for CSOs that were authorized through the JAB authorization path. We decided to

[3]Because the selection was based on a nongeneralizable sample, the results cannot be used to make inferences about all agencies and CSPs that had pursued FedRAMP authorizations.

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

include CSOs that had been issued an authorization through both paths, as they include different steps, which could potentially impact the costs and the associated challenges. We ensured that our sample included at least two CSPs that were small businesses. Further, we selected five additional CSPs based on the CSOs that agencies had used the most as of February 2023.

For the first objective, we analyzed FedRAMP Marketplace data to determine the extent to which agencies used FedRAMP authorizations for CSOs as of April 2023. In addition, we analyzed the data to determine how often agencies leverage authorizations for the various types of cloud services (e.g., cloud service model and risk impact level). Further, we analyzed OMB data on agencies' use of cloud services, including cloud services that were not FedRAMP authorized. We did not independently verify the data. Finally, we analyzed the questionnaire responses from selected agencies regarding their use of CSOs that were not FedRAMP authorized, including their reported reasons for using them.

To assess the reliability of the FedRAMP Marketplace data, we reviewed the fields for omissions, outliers, or obvious errors. In cases where we found possible errors or discrepancies, we followed-up with the FedRAMP PMO to obtain additional clarification. We determined that the data were sufficiently reliable for the purposes of discussing agencies' use of FedRAMP authorized cloud services, including the types of cloud services.

In addition, to assess the reliability of OMB's data on agencies' use of cloud services, we reviewed the fields for omissions, outliers, or obvious errors. We also interviewed OMB and FedRAMP PMO officials to discuss the data, including how they obtained and reviewed it. We determined that the data were sufficiently reliable for the purposes of identifying the number of agencies that self-reported that they were using cloud services that were not FedRAMP authorized.

However, we identified outliers in the number of cloud services that agencies reported that they used. These outliers were likely due to agencies that may have reported the data differently. In addition, due to omissions in the data (e.g., agencies that did not report the specific CSO that they were using), OMB was not able to determine whether agencies were using FedRAMP authorized CSOs for many of the reported cloud services. As such, we determined that the data identifying the total number of cloud services used by federal agencies and data identifying the total number of cloud services used by agencies that were not FedRAMP authorized were not sufficiently reliable for the purposes of this report.

For the second objective, we analyzed agencies' and CSPs' questionnaire responses on the reported costs incurred in pursuing authorizations, including the factors that impacted the costs. We did not independently verify the costs identified by the agencies and CSPs. Further, we reviewed FedRAMP PMO and OMB documentation to determine what, if any, data they had collected on costs incurred by agencies and CSPs when pursuing FedRAMP authorizations.

To assess the reliability of the cost data identified by the agencies and CSPs, we reviewed the fields for omissions, outliers, or obvious errors. In cases where we found possible errors or discrepancies, we followed-up with individual agencies and CSPs, as appropriate, to obtain additional clarification. We determined that the data were sufficiently reliable for the purposes of discussing the costs identified by the agencies and CSPs, including the types of costs. However, we found that agencies and CSPs did not use a consistent method for tracking the costs. For example, they used different factors to determine their costs. As a result, we determined that selecting additional agencies and CSPs would not provide us with meaningful data on the actual costs incurred.

For the third objective, we analyzed agencies' and CSPs' questionnaire responses to identify the most commonly reported challenges. Specifically, we assessed and categorized the challenges and totaled the number of times each challenge was cited by agency officials and CSP representatives. In order to identify the key challenges, we selected challenges that were mentioned by three or more agencies or CSPs. In addition, we reviewed OMB and FedRAMP PMO documentation (e.g., survey results) regarding any challenges that they had identified. Further, we reviewed FedRAMP PMO's and OMB's strategies and plans (e.g., FedRAMP PMO Fiscal Year 2023 Strategy), including their status in implementing them. We then compared these strategies and plans to the key challenges to identify which challenges the agencies had plans to address, and where there were gaps, if any. Because the selection of agencies and CSPs was based on a nongeneralizable sample, the results cannot be used to make inferences about the challenges faced by all agencies and CSPs that had pursued FedRAMP authorizations.

For each of the objectives, we supplemented the information obtained from our analyses by interviewing knowledgeable agency officials responsible for FedRAMP authorizations from GSA and OMB. In addition, we interviewed officials from the selected agencies and representatives from the selected CSPs to obtain additional information regarding their responses to the questionnaire, as needed.

We conducted this performance audit from January 2023 to January 2024 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Comments from the General Services Administration

DocuSign Envelope ID: 9DF6174D-328E-4C09-8804-040ED55899A5

GSA

The Administrator

December 18, 2023

The Honorable Gene L. Dodaro
Comptroller General of the United States
U.S. Government Accountability Office
Washington, DC 20548

Dear Comptroller General:

The U.S. General Services Administration (GSA) appreciates the opportunity to review and comment on the draft report, "Federal Authorization Program Usage Increasing, but Challenges Need to Be Fully Addressed" (GAO-24-106591). We agree with the findings and recommendation, and will take appropriate action.

If you have any additional questions or concerns, please contact me or Gianelle E. Rivera, Associate Administrator, Office of Congressional and Intergovernmental Affairs, at (202) 501-0563.

Sincerely,

Robin Carnahan
Administrator

cc: David Hinchman, Director, Information Technology and Cybersecurity

U.S. General Services Administration
1800 F Street NW
Washington, DC 20405
www.gsa.gov

Text of Appendix II: Comments from the General Services Administration

December 18, 2023

The Honorable Gene L. Dodaro Comptroller General of the United States

U.S. Government Accountability Office Washington, DC 20548

Dear Comptroller General:

The U.S. General Services Administration (GSA) appreciates the opportunity to review and comment on the draft report, "Federal Authorization Program Usage Increasing, but Challenges Need to Be Fully Addressed" (GAO-24-106591). We agree with the findings and recommendation, and will take appropriate action.

If you have any additional questions or concerns, please contact me or Gianelle E. Rivera, Associate Administrator, Office of Congressional and Intergovernmental Affairs, at (202) 501-0563.

Sincerely,

Robin Carnahan Administrator

cc: David Hinchman, Director, Information Technology and Cybersecurity

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

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

Staff Acknowledgments

In addition to the contact named above, the following staff made key contributions to this report: Neelaxi Lakhmani (Assistant Director), Scott Borre (Analyst in Charge), Justin Booth, Christopher Businsky, Brandon Cox, Kristi Dorsey, Rebecca Eyler, Hiama Halay, Sejal Sheth, and Andrew Stavisky.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Phone

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

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

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

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

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

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548