



December 2019

CLOUD COMPUTING SECURITY

Agencies Increased
Their Use of the
Federal Authorization
Program, but
Improved Oversight
and Implementation
Are Needed

Why GAO Did This Study

Federal agencies use internet-based (cloud) services to fulfill their missions. GSA manages FedRAMP, which provides a standardized approach to ensure that cloud services meet federal security requirements. OMB requires agencies to use FedRAMP to authorize the use of cloud services.

GAO was asked to review FedRAMP. The objectives were to determine the extent to which 1) federal agencies used FedRAMP to authorize cloud services, 2) selected agencies addressed key elements of the program's authorization process, and 3) program participants identified FedRAMP benefits and challenges. GAO analyzed survey responses from 24 federal agencies and 47 cloud service providers. GAO also reviewed policies, plans, procedures, and authorization packages for cloud services at four selected federal agencies and interviewed officials from federal agencies, the FedRAMP program office, and OMB.

What GAO Recommends

GAO is making one recommendation to OMB to enhance oversight, two to GSA to improve guidance and monitoring, and 22 to the selected agencies, including GSA. GSA and HHS agreed with the recommendations, USAID generally agreed, EPA generally disagreed, and OMB neither agreed nor disagreed. GAO revised four recommendations and withdrew one based on new information provided; it maintains that the remaining recommendations are warranted.

View [GAO-20-126](#). For more information, contact Gregory C. Wilshusen at 202-512-6244 or WilshusenG@gao.gov.

CLOUD COMPUTING SECURITY

Agencies Increased Their Use of the Federal Authorization Program, but Improved Oversight and Implementation Are Needed

What GAO Found

The 24 federal agencies GAO surveyed reported using the Federal Risk and Authorization Management Program (FedRAMP) for authorizing cloud services. From June 2017 to July 2019, the number of authorizations granted through FedRAMP by the 24 agencies increased from 390 to 926, a 137 percent increase. However, 15 agencies reported that they did not always use the program for authorizing cloud services. For example, one agency reported that it used 90 cloud services that were not authorized through FedRAMP and the other 14 agencies reported using a total of 157 cloud services that were not authorized through the program. In addition, 31 of 47 cloud service providers reported that during fiscal year 2017, agencies used providers' cloud services that had not been authorized through FedRAMP. Although the Office of Management and Budget (OMB) required agencies to use the program, it did not effectively monitor agencies' compliance with this requirement. Consequently, OMB may have less assurance that cloud services used by agencies meet federal security requirements.

Four selected agencies did not consistently address key elements of the FedRAMP authorization process (see table). Officials at the agencies attributed some of these shortcomings to a lack of clarity in the FedRAMP guidance.

Agency Implementation of Key Elements of the FedRAMP Authorization Process

Element	HHS	GSA	EPA	USAID
Control implementation summaries identified security control responsibilities	●	●	●	●
Security plans addressed required information on control implementation	◐	◐	◐	●
Security assessment reports summarized results of control tests	◐	◐	◐	●
Remedial action plans addressed required information	◐	◐	◐	◐
Cloud service authorizations prepared and provided to FedRAMP Program Office	◐	●	◐	◐

Legend: ● fully addressed the element ◐ partially addressed the element

FedRAMP = Federal Risk and Authorization Management Program; HHS = Department of Health and Human Services; GSA = General Services Administration; EPA = Environmental Protection Agency; USAID = U.S. Agency for International Development
Source: GAO analysis of agency documentation| GAO-20-126

Program participants identified several benefits, but also noted challenges with implementing the FedRAMP. For example, almost half of the 24 agencies reported that the program had improved the security of their data. However, participants reported ongoing challenges with resources needed to comply with the program. GSA took steps to improve the program, but its FedRAMP guidance on requirements and responsibilities was not always clear and the program's process for monitoring the status of security controls over cloud services was limited. Until GSA addresses these challenges, agency implementation of the program's requirements will likely remain inconsistent.

Contents

Letter		1
	Background	6
	The FedRAMP Security Assessment Framework Outlines Key Artifacts for Authorizing Cloud Services	12
	Agencies Increased Their Use of FedRAMP, but Many Continued to Use Cloud Services Not Authorized through FedRAMP	15
	Selected Agencies Did Not Consistently Address Key Elements of FedRAMP's Authorization Process	20
	Program Participants Reported Improved Security and other Benefits, but also Identified Challenges	30
	Conclusions	45
	Recommendations for Executive Action	46
	Agency Comments and Our Evaluation	49
Appendix I	Objectives, Scope, and Methodology	55
Appendix II	FedRAMP Roles and Responsibilities	61
Appendix III	FedRAMP Milestones	62
Appendix IV	Comments from the General Services Administration	63
Appendix V	Comments from the Department of Health and Human Services	65
Appendix VI	Comments from the Environmental Protection Agency	70
Appendix VII	Comments from the U.S. Agency for International Development	73

Appendix VIII	Comments from the Department of Veterans Affairs	78
Appendix IX	Comments from the Social Security Administration	79
Appendix X	GAO Contact and Staff Acknowledgments	80

Tables

Table 1: Key Elements of the FedRAMP Authorization Process	13
Table 2: Extent to Which Selected Agencies' System Security Plans Addressed Key Information	23
Table 3: Extent to Which Selected Agencies' Security Assessment Reports (SAR) Summarized Results of Control Tests	25
Table 4: Extent to Which Selected Agencies' Remedial Action Plans Included Required Information	27
Table 5: Selected Agencies Prepared and Provided Authorizations to the FedRAMP Program Management Office (PMO)	29
Table 6: Roles and Responsibilities of FedRAMP Governance Entities	61

Figures

Figure 1: Number of Federal Risk and Authorization Management Program (FedRAMP) Authorizations issued by the 24 Chief Financial Officers Act Agencies from June 2017 through July 2019	16
Figure 2: Number of FedRAMP Authorizations by Cloud Service and by Agency	17
Figure 3: Surveyed Agencies' Responses on Whether FedRAMP Made Their Data in Cloud Environments More or Less Secure	31
Figure 4: Responding Federal Agencies' List of Beneficial Federal Risk and Authorization Management Program (FedRAMP) Elements	34

Figure 5: Surveyed Cloud Service Providers (CSP) List of Beneficial Federal Risk and Authorization Management Program (FedRAMP) Elements	37
Figure 6: Federal Risk and Authorization Management Program (FedRAMP) Key Events, December 2011-June 2018	62

Abbreviations

ATO	authorization to operate
CFO	Chief Financial Officers Act of 1990
CIS	Control Implementation Summary
CIO	chief information officer
CSP	cloud service provider
DHS	Department of Homeland Security
DOD	Department of Defense
EPA	Environmental Protection Agency
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Modernization Act of 2014
GSA	General Services Administration
HHS	Department of Health and Human Services
IT	information technology
IaaS	Infrastructure as a Service
JAB	Joint Authorization Board
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PaaS	Platform as a Service
PMO	Program Management Office
SaaS	Software as a Service
P-ATO	provisional authorization to operate
SAR	security assessment report
SSP	system security plan
3PAOs	third-party assessment organizations
TIC	Trusted Internet Connection
USAID	United States Agency for International Development

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



December 12, 2019

Congressional Requesters

Over the past decade, federal agencies have increasingly used internet-based computing services (commonly referred to as cloud services) to address their information technology needs. According to the Office of Management and Budget (OMB), cloud services offer agencies a number of benefits, including reduced information technology (IT) procurement and operating costs, and increased efficiency and effectiveness in delivering services.

However, as we have previously reported, the use of cloud computing also poses cybersecurity risks.¹ These risks arise when agencies and cloud service providers do not effectively implement security controls over cloud services. Weaknesses in these controls could lead to vulnerabilities affecting the confidentiality, integrity, and availability of agency information.

To facilitate the adoption and use of cloud services, OMB established the Federal Risk and Authorization Management Program (FedRAMP) in 2011. The program is intended to provide a standardized approach for selecting and authorizing the use of cloud services that meet federal security requirements. Managed by the General Services Administration (GSA), the program aims to ensure that cloud computing services have adequate information security, while also eliminating duplicative efforts and reducing operational costs.

FedRAMP establishes security requirements and guidelines that are intended to help secure cloud computing environments used by agencies and meet the provisions of the *Federal Information Security Modernization Act of 2014* (FISMA) and implementing guidance.²

¹GAO, *Information Security: Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing*, [GAO-10-513](#) (Washington, D.C.: May 27, 2010).

²The *Federal Information Security Modernization Act of 2014* (FISMA 2014), enacted as Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014), largely superseded the *Federal Information Security Management Act of 2002* (FISMA 2002), enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this report, FISMA refers both to FISMA 2014 and to those provisions of FISMA 2002 that were either incorporated into FISMA 2014 or were unchanged and continue in full force and effect.

FedRAMP's requirements and guidelines specify the actions agencies and cloud service providers should take in order to authorize cloud services through the program. Further, OMB requires agencies to authorize information systems prior to their operation and periodically thereafter. This requirement also applies to the use of cloud services.³ OMB required that by June 2014, all executive branch agencies use FedRAMP for authorizing all cloud services.⁴

You requested that we review the progress and challenges associated with the FedRAMP program. Our objectives were to determine the extent to which (1) federal agencies used FedRAMP to authorize the use of cloud services, (2) selected agencies addressed key elements of the program's authorization process, and (3) program participants identified FedRAMP benefits and challenges.

To address the first objective, we examined data reported by GSA to determine whether FedRAMP authorizations for the 24 agencies covered by the *Chief Financial Officers (CFO) Act of 1990*⁵ (hereafter referred to as the CFO Act agencies) increased or decreased in fiscal year 2019 compared to the number of authorizations issued in fiscal year 2017. In

³Office of Management and Budget, *Managing Information as a Strategic Resource*, Circular A-130 (Washington, D.C.: July 2016). The circular mentions that FISMA requires each agency to provide information security for the information and "information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source." This includes services that are either fully or partially provided, including agency-hosted, outsourced, and cloud-based solutions.

⁴Office of Management and Budget, *Security 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 two years from the time FedRAMP became operational in June 2012, to comply with those requirements.

⁵The 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)).

addition, we administered web-based surveys to the 24 CFO Act agencies⁶ and to 83 cloud service providers⁷ participating in FedRAMP⁸ to gather information about their use of the program.⁹ We also interviewed knowledgeable officials from the 24 agencies, the FedRAMP Program Management Office (PMO), and the Joint Authorization Board (JAB)¹⁰ about the extent to which agencies were using the program. Further, we reviewed OMB's annual guidance on FISMA to agencies and agencies' annual FISMA reports to determine the reporting of FedRAMP usage.¹¹

To address the second objective, we selected four agencies from the 24 CFO Act agencies.¹² These agencies were the Department of Health and Human Services (HHS), the Environmental Protection Agency (EPA), GSA, and the United States Agency for International Development (USAID). Because HHS is a large federated agency, we selected three of

⁶On June 1, 2018, we sent the web-based survey to the 24 CFO Act agencies.

⁷On April 30, 2018, we sent the web-based survey to the 83 cloud service providers.

⁸The FedRAMP Program Management Office (PMO), which is part of GSA, identified these 83 cloud service providers as participating in the FedRAMP Program as of January 24, 2018. GAO reached out to each agency and cloud service provider to determine the correct point of contact was provided a copy of the survey. In addition, the CISO or CIO of the agency was required to review and sign-off on the survey before the point of contact could submit the survey as completed.

⁹The 24 agencies completed the survey. We also received completed surveys from 47 of the 83 cloud service providers. Not all survey respondents provided answers to all survey questions. The results of these surveys are not generalizable to all federal agencies or all cloud service providers.

¹⁰The Joint Authorization Board (JAB) is the primary governance and decision-making body for the FedRAMP program. The JAB reviews and provides provisional security authorizations of cloud solutions using a standardized baseline approach. The chief information officers from the Department of Defense, Department of Homeland Security, and General Services Administration serve on the board.

¹¹For this report, we interviewed JAB officials including the technical representatives from the General Service Administration, Department of Defense, and Department of Homeland Security.

¹²To select the four agencies, we ranked the 24 federal agencies based on the highest to lowest number of FedRAMP PMO service authorizations granted during FY 2017. We then divided the 24 agencies into three groups of eight agencies. We selected agencies with the highest number of authorizations in each group. Since the two agencies in the third group with the highest number of authorizations had the same number of services authorized, we selected both agencies. To avoid a duplication of our efforts, we excluded DOD because another GAO team was reviewing the department's cloud-related efforts, which also included FedRAMP.

its operating divisions for a more detailed review. These three divisions were the Centers for Disease Control and Prevention (CDC), the Centers for Medicare and Medicaid Services (CMS), and the National Institutes of Health (NIH). We selected these divisions based on their extensive usage of cloud service providers authorized through FedRAMP.

From these agencies, we selected 10 authorization packages for IT systems that the agencies reported as being supported by cloud services approved through FedRAMP.¹³ We selected these services and their corresponding authorization packages based on data from the PMO which indicated that, as of June 15, 2017, these cloud services were the most used by the 24 agencies. Our findings related to the four agencies and 10 authorization packages we selected, but were not generalizable to all of the agencies in our review.

To determine whether the four selected agencies were effectively implementing the FedRAMP authorization process, we collected authorization artifacts, including (1) control implementation summaries, (2) system security plans, (3) security assessment reports, (4) remedial action plans, and (5) letters authorizing the systems using cloud services. We then compared these documents to OMB's guidance on cloud computing; National Institute of Standards and Technology (NIST) Special Publication 800-53; and PMO guidance on using FedRAMP.¹⁴ We also reviewed and compared cloud service provider documentation to agency documentation to identify whether there were inconsistencies between the agency and cloud service provider responsibilities for implementing security controls. Using a risk-based approach, we identified and selected 24 security controls from the 97 core controls identified in FedRAMP guidance¹⁵ and determined whether these controls

¹³To select the specific agency systems to review, we sent agencies or their specified operational divisions a list of cloud services that the FedRAMP PMO reported that the agencies were using as of June 15, 2017, and asked them to specify the systems that relied on the cloud services authorized and approved through FedRAMP.

¹⁴National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, SP 800-53, Revision 4 (Gaithersburg, MD: April 2013).

¹⁵FedRAMP, *FedRAMP Security Assessment Framework Version 2.1* (Washington, D.C.: Dec. 4, 2015). We reviewed FY 2017 authorizations which followed the 2015 FedRAMP security assessment framework. The 2015 FedRAMP security assessment framework was updated in 2017. The framework stated that core controls are security controls that must be re-tested at least annually for continuous monitoring.

were addressed in the selected agencies' and components' system security plans.¹⁶

Further, we interviewed relevant agency officials to obtain their views on the effectiveness of the program's authorization process. We also interviewed officials and obtained documentary evidence from the PMO and JAB to obtain information on their process for reviewing authorization packages.

For the third objective, we reviewed the responses from the 24 CFO Act agencies and 47 cloud service providers to our two surveys to identify information on the usefulness of FedRAMP policies, procedures, and guidance, as well as the benefits, challenges, and areas of improvement. In addition, we interviewed officials from the FedRAMP PMO, JAB, and the 24 CFO Act agencies, including the four selected agencies and their operational divisions.

To assess the reliability of the data used to select agencies for our review and other data used to address the three objectives, we reviewed the following:

- FedRAMP PMO points of contact list for active cloud service providers and federal agency users of FedRAMP,
- FedRAMP PMO data on the 24 CFO Act agencies' fiscal years 2017, 2018, and 2019 JAB and agency authorizations,
- FedRAMP PMO data on cloud service provider participation and agency usage of FedRAMP as of June 15, 2017,
- Agency inventories of systems relying on selected cloud services,
- Cloud service provider authorization documentation contained within secure website portals,
- Cloud service provider and agency reported third-party assessment organizations' security assessment reports, and
- Agency plans of actions and milestones.

We evaluated the materiality of the data to our audit objectives and assessed the data reliability by reviewing related documents, interviewing

¹⁶We selected a nongeneralizable sample of controls that included those reviewed by the FedRAMP PMO and the JAB.

knowledgeable agency officials, and reviewing internal controls such as agency policies and procedures. Based on our assessment of this information, we concluded that the data were sufficiently reliable for the purposes of our reporting objectives. See appendix I for additional details on our objectives, scope, and methodology.

We conducted this performance audit from November 2016 to December 2019 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

Federal agencies and our nation's critical infrastructures rely on information technology systems that are highly complex and dynamic, technologically diverse, and often geographically dispersed. This complexity increases the difficulty in identifying, managing, and protecting the numerous operating systems, applications, and devices comprising their systems and networks.

Further, federal systems and networks are at an increased risk of attack. This is due to those systems often being interconnected with other internal and external systems and networks, including the internet. Cloud computing relies on internet-based interconnectivity and resources to provide computing services to customers, while intending to free customers from the burden and costs of maintaining the underlying infrastructure.

As federal agencies increasingly use cloud computing to perform their missions, the implementation of effective information security controls becomes more important. The effective implementation of a standardized process for securing cloud environments could reduce risks to agency systems and information maintained on an agency's behalf.

The *Federal Information Security Modernization Act of 2014* (FISMA) was enacted to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. The act requires federal

agencies to develop, document, and implement an information security program, and evaluate the program's effectiveness.¹⁷

FISMA also requires OMB to develop and oversee the implementation of policies, principles, standards, and guidelines on information security in federal agencies, except with regard to national security systems. The law assigns OMB the responsibility of requiring agencies to identify and provide information security protections commensurate with assessments of risk to their information and information systems.

In addition to implementing an agencywide security program, FISMA requires agencies to ensure the security of information and systems maintained by or on behalf of the agency. The law also applies to systems used or operated by a contractor or other organization on behalf of the agency, such as IT resources provided via cloud services.

In December 2010, OMB issued a plan for improving IT management that included provisions for a decision framework to migrate IT services to cloud environments.¹⁸ Since then, OMB has developed cloud computing requirements, issued a number of cloud-related documents, and established FedRAMP. OMB cloud-related documents include:

- *Federal Cloud Computing Strategy*, which was intended to accelerate the government's use of cloud computing by requiring agencies to evaluate safe, secure cloud computing options before making any new investments.¹⁹
- *Security Authorization of Information Systems in Cloud Computing Environments*, which established FedRAMP in December 2011.²⁰

¹⁷The *Federal Information Security Modernization Act of 2014* (Pub. L. No. 113-283, Dec. 18, 2014) largely superseded the *Federal Information Security Management Act of 2002* (FISMA 2002), enacted as Title III, *E-Government Act of 2002*, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002).

¹⁸Office of Management and Budget, *25 Point Implementation Plan to Reform Federal Information Technology Management* (Washington, D.C.: Dec. 9, 2010).

¹⁹Office of Management and Budget, *Federal Cloud Computing Strategy* (Washington, D.C.: Feb. 8, 2011).

²⁰Office of Management and Budget, *Security Authorization of Information Systems in Cloud Computing Environments* (Washington, D.C.: Dec. 8, 2011).

-
- 2019 *Federal Cloud Computing Strategy*, issued in June 2019,²¹ updates the 2011 Federal Cloud Computing Strategy and provides agencies with additional guidance on implementing cloud solutions and emphasizes cloud security as one of the three pillars of successful cloud adoption.

In addition, the FedRAMP PMO established a framework for authorizing cloud services and guidance to help participants, including all agencies, implement it.²² According to the program management office, the framework is based on NIST guidance that agencies are supposed to follow.²³ In addition to the framework, the program management office issued guidance on how agencies can leverage²⁴ existing security authorization packages.²⁵

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

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

- **Infrastructure as a Service (IaaS).** The cloud service provider 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 cloud service provider delivers and manages the infrastructure, operating system, and programming tools and services, which the agency can use to create applications.

²¹Office of Management and Budget, *Federal Cloud Computing Strategy* (Washington, D.C.: June 24, 2019).

²²FedRAMP Program Management Office, *FedRAMP Security Assessment Framework Version 2.4* (Washington, D.C.: Nov. 15, 2017).

²³OMB Circular A-130 states agencies must apply the NIST standards and guidelines.

²⁴According to OMB, leveraged authorizations can be used when an agency chooses to accept some or all of the information in an existing authorization package generated by another agency based on the need to use the same information resources (e.g., information system or services provided by the system).

²⁵FedRAMP Agency Guide For FedRAMP Authorizations: *How to Functionally Reuse an Existing Authorization Version 2.0* (Washington, D.C.: Dec. 7, 2017).

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

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

- **Private cloud.** The service is set up specifically for one organization, although there may be multiple customers within that organization and the cloud may exist on or off the customer's premises.
- **Community cloud.** The service is set up for organizations with similar requirements. The cloud may be managed by the organizations or a third-party and may exist on or off the organization's premises.
- **Public cloud.** The service is available to the general public and is owned and operated by the service provider.
- **Hybrid cloud.** The service is a composite of two or more of the three deployment models (private, community, or public) that are bound together by technology that enables data and application portability.

These deployment models differ from each other in the number of consumers they serve, the nature of various consumers' data that may be present in the cloud environment, and the amount of control consumers have over their data. A private cloud can allow for its consumers to have ultimate control in selecting who has access to that cloud environment. Community clouds and hybrid clouds allow for a mixed degree of consumers' control and knowledge of other consumers. A public cloud allows access by all interested consumers, but, in doing so, should not allow one consumer who uses it to know or control data that belong to other consumers of that environment.

FedRAMP Is a Government-wide Program for Authorizing Cloud Services

Established by OMB and managed by GSA, the FedRAMP program is intended to provide a standardized approach to securing systems, assessing security controls, and continuously monitoring cloud services used by federal agencies.²⁶ 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/service for federal agencies.

The program’s key participants are the FedRAMP PMO, JAB, federal agencies, cloud service providers, and third-party assessor organizations.

- **FedRAMP PMO.** FedRAMP’s PMO 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, creating guidance and templates for agencies and cloud service providers to use for developing, assessing, authorizing, and continuously monitoring cloud services per federal requirements (e.g., FISMA).
- **JAB.** The JAB is made up of chief information officers from the Department of Defense (DOD), DHS, and GSA. It is the primary governing and decision-making body of the program. The JAB is responsible for defining and establishing FedRAMP baseline security controls and accreditation criteria for third-party assessment organizations. The JAB is also responsible for issuing a provisional authorization to operate (P-ATO) for cloud services it determines will be leveraged across most of the federal government.
- **Federal agencies.** They are consumers and, in some cases, providers of cloud services. Agencies are responsible for ensuring that cloud services which process, transmit, or store government information, use FedRAMP’s baseline security controls before they issue subsequent authorizations for using those cloud services.

²⁶Private cloud deployments intended for single organizations and implemented fully within federal facilities are exempt from the FedRAMP requirements.

-
- **Cloud service providers (CSP).** These providers include commercial firms and some federal agencies that offer cloud services to agencies.²⁷ Providers are required to meet the FedRAMP security requirements and implement the program's baseline security controls.²⁸ Providers work with an independent third-party assessment organization to conduct an initial system assessment, create security assessment documentation per the program's requirements, and comply with federal requirements for incident reporting, among others.
 - **Third-party assessment organizations.** These FedRAMP accredited assessors perform initial and periodic assessments of cloud providers' controls to ensure they meet the program's requirements. In addition, these assessors must be accredited through FedRAMP if they are assessing a cloud provider seeking a provisional authorization from the JAB. For details on the roles and responsibilities of other entities involved with the program, see table 6 in appendix II.

²⁷Federal agencies can act as a cloud service provider for other agencies. For example, the United States Department of Agriculture, the Department of the Treasury, and the General Services Administration are cloud service providers for other agencies, according to their survey responses.

²⁸According to NIST, 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 200—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; 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).

The FedRAMP Security Assessment Framework Outlines Key Artifacts for Authorizing Cloud Services

In December 2015, the FedRAMP PMO developed a security assessment framework that is to be followed by the cloud service providers (providers) and agencies seeking to authorize cloud services through the program.²⁹ In addition to outlining roles and responsibilities, the framework provides agencies and cloud service providers with guidance on elements key to issuing authorizations for using cloud services through the program. These elements are critical to developing the information system or cloud service authorization package. Authorization packages include, but are not limited to the following artifacts: a control implementation summary, the security plan, the security test plan and assessment report, and remedial actions plan. These artifacts are described in table 1.

²⁹According to the FedRAMP program management office, the FedRAMP security assessment framework is compliant with FISMA and is based on NIST Special Publication 800-37. National Institute of Standards and Technology, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, SP 800-37 (Gaithersburg, MD: February 2010).

Table 1: Key Elements of the FedRAMP Authorization Process

Artifact	Purpose	Role/Responsibility
Control Implementation Summary (CIS)	Specifies security responsibilities for the agencies and providers.	Agency: Reviews the summary to ensure that control responsibilities assigned to the agency or shared with the cloud service provider are accurately defined. Cloud Service Provider (CSP): Provides the agency with the CIS identifying the controls it and the agency has responsibility for implementing.
System Security Plan (SSP)	Documents the security controls that need to be implemented to meet FedRAMP's requirements	Agency: Reviews the CSP plan to ensure that responsibilities outlined in CIS are consistent. Creates an agency SSP to include the controls for which the agency has sole responsibility or a shared responsibility with the CSP. Uses FedRAMP or NIST guidance for documenting their control responsibilities in an agency SSP. CSP: Creates the plan that documents the controls for which the CSP has responsibility for implementing or a shared responsibility with the agency.
Security Assessment Report (SAR)	Documents results of control tests and control effectiveness.	Agency: Reviews the report of the CSP's environment to determine if risks identified by the independent third-party assessor are acceptable. Assesses controls for which the agency has responsibilities for implementing. Tests controls for which it has responsibility and documents them in a SAR. CSP: Works with an independent assessor that test's the provider's cloud service for weaknesses. Accredited Third-Party Assessor (3PAO)/Independent Assessor (IA): Tests the security controls of the cloud service for weaknesses and produces the report for the CSP and agency to review.
Remedial Action Plan	Lists cloud service deficiencies; identifies responsibilities for addressing deficiencies; and cites resources and planned dates for mitigating deficiencies.	Agency: Reviews remedial actions for control deficiencies identified with the cloud service to determine risk and whether it is acceptable for authorizing the cloud service. Prepares remedial action plans for mitigating control deficiencies the agency has responsibility for implementing. Maintains remedial action plans and corrects control deficiencies for which it has responsibility. CSP: Maintains remedial action plans and mitigates control deficiencies identified with its service. CSPs develop remedial action plans based on the SAR provided by 3PAOs or IA.

Legend: FedRAMP = Federal Risk and Authorization Management Program; NIST = National Institute of Standards and Technology.

Source: GAO summary based on FedRAMP and NIST guidance. | GAO-20-126

Agencies Have Two Options for Issuing Authorizations

FedRAMP provides agencies with two options for authorizing cloud services. The first option, called a JAB authorization, involves the agency authorizing the cloud service based on a provisional authorization³⁰ issued by the board. The second option, called an agency authorization, involves the agency issuing an authorization after either sponsoring³¹ a cloud service provider through FedRAMP, or by leveraging³² another agency's FedRAMP authorization of that cloud service provider.

Using either of these options, the agency is to review the authorization package for that cloud service prior to issuing its authorization. In reviewing the package, the agency is to consider the cloud service's system impact level (low impact, moderate impact, or high impact),³³ and deployment model, among other things, to help determine which authorization option is more appropriate.

After an agency has reviewed the package and made a risk-based decision to authorize a cloud service for use, it is to formally document this decision in an authorization letter. The agency official authorizing the

³⁰A provisional authorization is an initial statement of risk and approval of an authorization package by the Joint Authorization Board pending the issuance of a final authorization to operate by the executive department or agency acquiring the cloud service.

³¹"Sponsoring" means an agency works with a cloud service provider to issue the provider's initial agency authorization through FedRAMP. The FedRAMP PMO reviews the complete package (along with the signed ATO) and issues the designation of FedRAMP authorized.

³²"Leveraging" a FedRAMP authorized cloud product or service is when an agency uses another agency ATO, including all supporting documentation, when making a risk-based decision to grant an agency ATO. This provides an agency the ability to reuse authorization packages to acquire cloud products or services from a cloud service provider listed in the FedRAMP Marketplace.

³³According to NIST's publication FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, there are three impact levels for systems. Low Impact systems are most appropriate where the loss of confidentiality, integrity, and availability would result in limited adverse effects on an agency's operations, assets, or individuals. Moderate Impact systems are most appropriate where the loss of confidentiality, integrity, and availability would result in serious adverse effects on an agency's operations, assets, or individuals. Serious adverse effects could include significant operational damage to agency assets, financial loss, or individual harm that is not loss of life or physical. High Impact systems are usually related to law enforcement and emergency services systems, financial systems, health systems, and any other system where loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

cloud service must provide a copy of the letter to the FedRAMP PMO.³⁴ The PMO uses the information to verify agency use and keep other agencies informed of any changes to a provider's authorization.

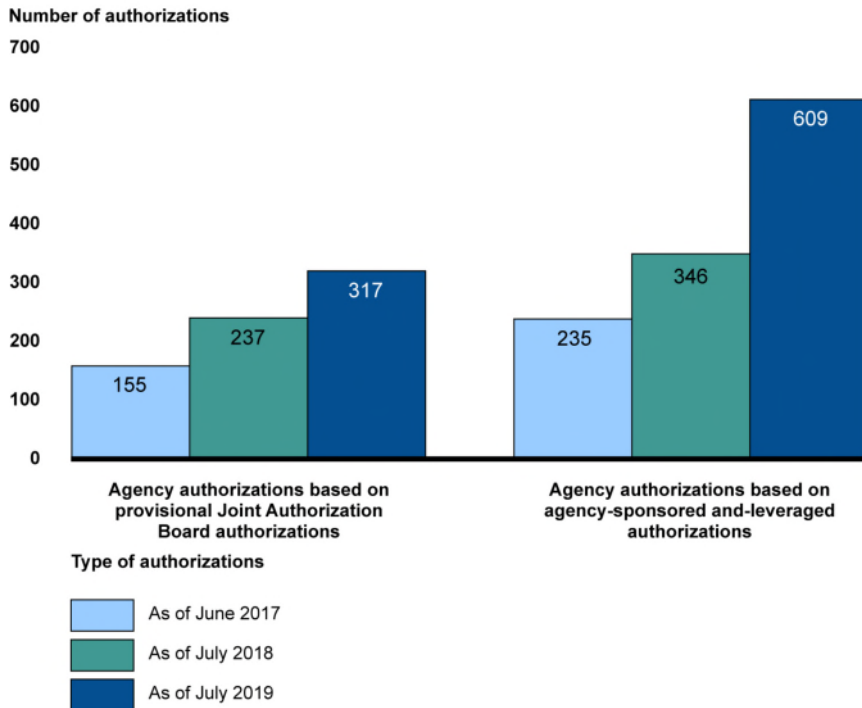
Agencies Increased Their Use of FedRAMP, but Many Continued to Use Cloud Services Not Authorized through FedRAMP

As of July 2019, all 24 CFO Act agencies participated in FedRAMP.³⁵ According to the program management office's documentation, from June 2017 through July 2019, these agencies' use of FedRAMP authorizations increased from 390 authorizations to 926 authorizations. Specifically, the number of JAB authorizations increased from 155 to 317—a 105 percent increase. Further, the total number of agency sponsored and –leveraged authorizations increased, from 235 to 609—a 159 percent increase. Figure 1 illustrates the increase in the number of FedRAMP authorizations for the 24 agencies from June 2017 through July 2019.

³⁴If an agency is sponsoring a cloud service, it must provide a copy of the authorization letter and package to the FedRAMP PMO. If an agency is reusing a JAB provisional authorization or an existing FedRAMP agency authorization, it only has to provide the PMO with only a copy of the authorization letter.

³⁵The 24 agencies' data on the total number of board provisional authorizations, agency-sponsored authorizations, and leveraged agency authorizations are based on voluntarily-provided authorization to operate letters that were submitted to the FedRAMP PMO by each agency. The 2017, 2018, and 2019 data were generated by the FedRAMP PMO on June 15, 2017; July 23, 2018; and July 23, 2019 respectively.

Figure 1: Number of Federal Risk and Authorization Management Program (FedRAMP) Authorizations issued by the 24 Chief Financial Officers Act Agencies from June 2017 through July 2019



Source: FedRAMP Program Management Office provided data. | GAO-20-126

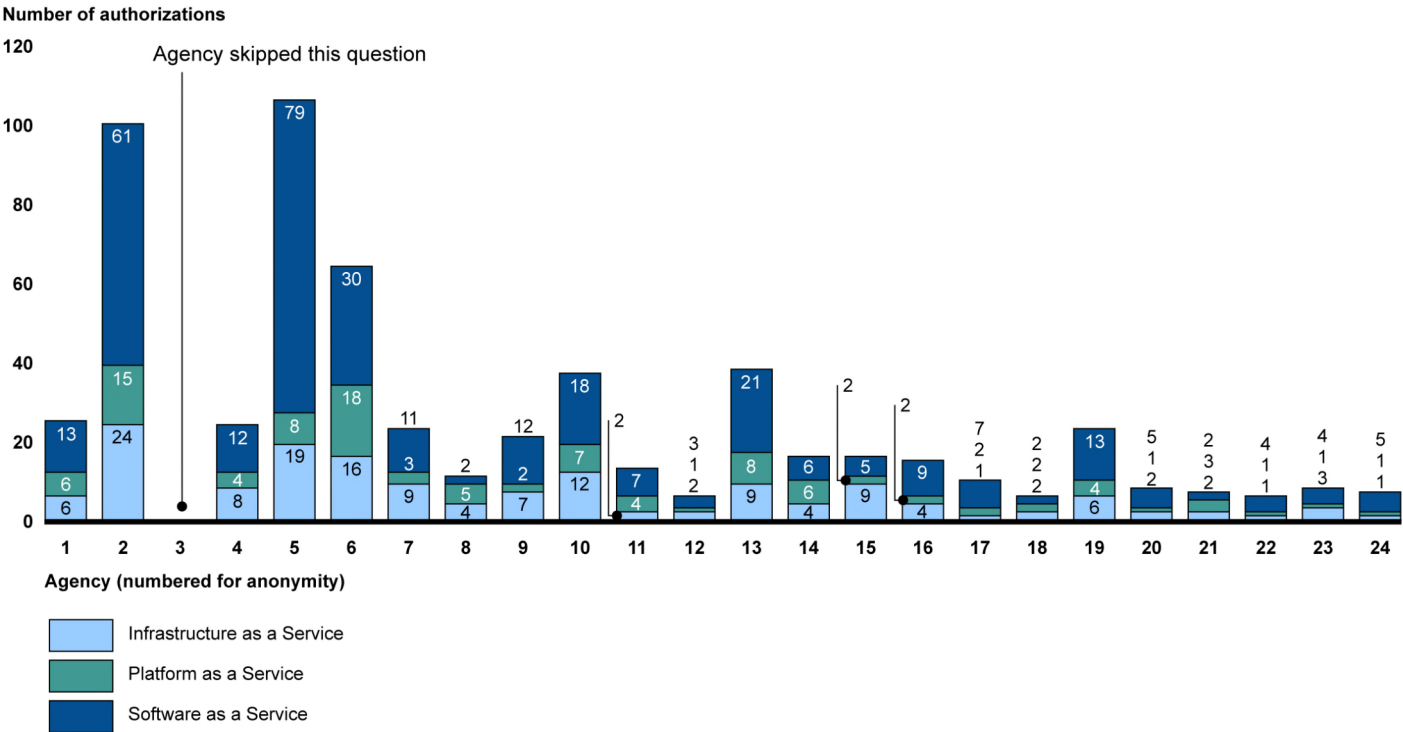
Note: The 24 Chief Financial Officers Act agencies are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, and Social Security Administration, and the United States Agency for International Development.

Agencies Reported a Higher Number of Authorizations for Software as a Service than for Other Cloud Services

Survey responses from 23 of 24 CFO Act agencies indicated that the highest number of cloud service authorizations through FedRAMP were for Software as a Service. Software as a Service accounted for 331 of the 590 reported authorizations or 56 percent. For the other two services, Infrastructure as a Service and Platform as a Service, agencies reported issuing 153 authorizations (26 percent) and 106 authorizations (18 percent), respectively. Figure 2, depicts the authorizations by agency and cloud service and shows that 18 of 23 agencies issued more

authorizations for Software as a Service than Platform as a Service or Infrastructure as a Service.³⁶

Figure 2: Number of FedRAMP Authorizations by Cloud Service and by Agency



Source: GAO analysis based on responses to GAO's agency survey. | GAO-20-126

Note: The 24 agencies that responded to our agency survey 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 United States Agency for International Development. The numbers in the X axis should not be attributed to a specific agency, as these responses were anonymous by design.

A cloud service may include one or more service models. These data were provided by the surveyed agencies, and GAO did not verify the responses for accuracy.

³⁶Two agencies issued an equal number of authorizations for Software as a Service and Platform as a Service. Two agencies had more authorizations for Platform as a Service than Software as a Service, and one agency had more authorizations for Infrastructure as a Service than Software as a Service. One agency did not respond to this question.

In addition, while agencies are consumers of cloud services, some agencies also serve as cloud service providers to other federal agencies. Four of 24 agencies reported that they served as cloud service providers to other federal agencies in FY 2017. All four agencies reported that their cloud services received authorizations that were approved through FedRAMP and used by other federal agencies. These four agencies reported a total of seven cloud services with an agency authorization and one cloud service with a provisional authorization from the JAB.

Agencies Reported Using Cloud Services That Were Not Authorized through FedRAMP

OMB required all agencies to use FedRAMP for authorizing cloud services by June 2014, and by June 2017, all of the 24 CFO Act agencies were using the program. However, the agencies also used cloud services that were not authorized through the program. In responding to our survey, the majority of the agencies (15 of 24) reported that they used cloud services that were not authorized through FedRAMP. For instance, one agency reported that it used 90 cloud services that were not authorized through FedRAMP and the other 14 agencies reported using a total of 157 cloud services that were not authorized through FedRAMP. Seven agencies responded that they only use cloud services authorized through FedRAMP. Two agencies did not provide a response for this question.

Agencies provided varying explanations for using cloud services that were not authorized through FedRAMP. For example, officials from two of the agencies stated that they were unable to identify providers authorized through the program that could meet their unique needs. An official from a third agency noted that the efforts to meet the program's requirements were labor-intensive and that it was too expensive for the providers to become compliant with FedRAMP. In addition, that official stated that providers did not want to pursue FedRAMP compliance unless they had enough demand from federal customers.

An official from a fourth agency stated that some of that agency's cloud services were considered to be private and, thus, did not need to be authorized through the program.³⁷ Nevertheless, according to that official, the agency performed its own authorization actions to ensure that FedRAMP requirements were met. In a similar example, an official at another agency noted that it took a significant amount of time for a

³⁷According to OMB, private cloud deployments intended for single organizations and implemented fully within federal facilities are exempt from the FedRAMP requirements.

provider to complete the FedRAMP process and that the agency had to issue its own authorization while the provider was going through the process. That authorization had not yet been approved through FedRAMP.

The survey responses of cloud service providers were consistent with the agencies' responses and indicated that multiple agencies were using cloud services that were not authorized or approved through FedRAMP.³⁸ For example, 31 of 47 providers that responded to our survey reported that, during FY 2017, agencies had used their cloud services and those services were not authorized by FedRAMP. According to one cloud service provider, agencies were using 30 of its cloud services that were not authorized through FedRAMP. Another cloud service provider reported that agencies were using nine of its cloud services that were not authorized through the program.

Officials from the FedRAMP program management office also provided several reasons why agencies did not use the program for all of their cloud services. For example, one PMO official indicated agencies had misperceptions of the program, its process, and resources required for a FedRAMP authorization. The official also specified that agencies did not use the program for all their cloud services because of internal resource constraints based on other competing agency priorities.

Based on our work, another potential reason that agencies authorize cloud services outside of the FedRAMP program is that OMB has not adequately monitored compliance with this requirement. As mentioned earlier, OMB has issued a number of policies encouraging agencies to adopt cloud computing solutions and requiring agencies to use FedRAMP for authorizing cloud services. Nevertheless, OMB has not monitored agencies' compliance or held agencies accountable for complying with the requirement to ensure that agencies are using the program to authorize their cloud services.

According to an OMB technical specialist, the office collects and reviews data from the FedRAMP Marketplace to monitor agencies' use of the

³⁸For this question in the CSP survey, providers referred to all federal agencies and did not focus their response to only the 24 agencies in our review.

program.³⁹ However, the office does not collect data on the extent to which federal agencies are using cloud services authorized outside of the program or oversee agencies' compliance with using FedRAMP. As a result, if OMB does not monitor or hold agencies accountable for using the FedRAMP program, OMB and federal agencies have reduced assurance that security controls required by the program are being consistently implemented. Additionally, OMB may lack information on agencies' needs for cloud services.

Selected Agencies Did Not Consistently Address Key Elements of FedRAMP's Authorization Process

Although the four selected agencies included key documents supporting FedRAMP's authorization process, they did not consistently include key information in those documents.⁴⁰ Specifically, these four agencies did not consistently or fully address required information in system security plans, security assessment reports, and remedial action plans. In addition, the agencies did not always prepare their authorizations approving the use of cloud services.

Agencies' Authorization Packages Included Control Implementation Summaries

FedRAMP recommends that agencies use the FedRAMP Control Implementation Summary (CIS) when leveraging cloud services for their systems.⁴¹ In addition, FedRAMP specifies that agencies are to use NIST guidance when addressing their individual or shared control implementation responsibilities when leveraging cloud services.

³⁹According to FedRAMP's program management office, the 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. The Marketplace also lists the third-party assessment organizations that have been approved to perform FedRAMP assessments.

⁴⁰The four agencies we selected for review were the Department of Health and Human Services (including the Centers for Disease Control and Prevention, the Centers for Medicare and Medicaid Services, and the National Institutes of Health); and the General Services Administration, Environmental Protection Agency, and United States Agency for International Development.

⁴¹The FedRAMP Control Implementation Summary (CIS) is a document that lists all the controls the cloud service provider is responsible for implementing, as well as the controls that the agency has responsibility for implementing.

All 10 authorization packages we reviewed contained a summary, which identified agencies' control implementation responsibilities as well as that of the cloud service providers.⁴²

Selected Agencies Did Not Consistently Document Required Information in System Security Plans

An objective of system security planning is to improve the protection of information system resources. A system security plan provides an overview of the security requirements for a system or cloud service and describes the controls that are in place or planned to meet those requirements. To identify controls that an agency will need to document on its security plan, the agency reviews the CIS which lists both the agency and CSP's security control responsibilities. Further, NIST guidelines state that federal agencies' system security plans should identify:

- an explicitly defined authorization boundary for the system,⁴³
- how the system operates in terms of mission and business processes,
- the security categorization of the system including supporting rationale,
- the operational environment of the system and connections to other information systems,
- the security controls in place or planned for meeting security requirements, including a rationale for supplementing controls, and
- a review and approval by the authorizing official or designated representative prior to plan implementation.⁴⁴

⁴²According to FedRAMP's PMO, agencies are to use the Control Implementation Summary to help identify the controls that the agencies have a primary or shared responsibility to implement. These controls and their implementation should be documented and described in security plans for agency systems that are supported by cloud services.

⁴³According to guidance from FedRAMP's PMO, an authorization boundary for cloud technologies should describe a cloud service's internal components and connections to external services and systems.

⁴⁴National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, SP-800-53, Revision 4 (Gaithersburg, MD: April 2013)

As shown in table 2, the four selected agencies had documented security plans for 10 systems. However, the agencies had not consistently addressed the required information in their plans.

Table 2: Extent to Which Selected Agencies' System Security Plans Addressed Key Information

Agency	Agency component	Selected system security plan ^a	Described authorization boundary	Described system operation in terms of mission and business processes	Identified security categorization and provided rationale	Identified operational environment and connections	Described the implementation of security controls	Reviewed and approved by authorizing official
HHS	CDC	System 1	◐	●	●	◐	◐	◐
	CMS	System 2	●	●	●	●	◐	●
		System 3	●	●	●	●	◐	●
	NIH	System 4	○	●	●	◐	◐	●
		System 5	○	●	●	◐	◐	●
GSA	No agency component	System 6	●	●	●	●	◐	◐
	No agency component	System 7	●	●	●	●	◐	◐
EPA	No agency component	System 8	●	●	●	●	◐	◐
	No agency component	System 9 ^b	◐	◐	●	●	◐	◐
USAID	No agency component	System 10	●	●	●	●	●	●

Legend:

- The agency system security plan addressed key NIST information.
- ◐ The agency system security plan partially addressed key NIST information.
- The agency system security plan did not address key NIST information.

HHS = Department of Health and Human Services; CDC = Centers for Disease Control and Prevention; CMS = Centers for Medicaid and Medicare Services; NIH = National Institutes of Health (CDC, CMS, and NIH are agency components of HHS); GSA = General Services Administration; EPA = Environmental Protection Agency; USAID = U.S. Agency for International Development.

Source: GAO analysis of agency documentation. | GAO-20-126

^aDue to sensitivity concerns, we substituted a numeric identifier for the system names.

^bSubsequent to our review of the system's security plan, EPA decommissioned System 9.

Note: We reviewed 24 core controls deemed as critical to protecting a cloud service, and whether agencies documented the implementation status of controls for which they were responsible.

As illustrated above, the security plans for the nine selected systems did not fully address all required information. For example, three plans

partially identified the operational environment of the system, such as identifying external connections which could include the cloud service the agency system was leveraging. In addition, nine plans did not fully address the extent to which security controls were in place, including those listed as the agency's responsibility. Further, agencies did not provide complete support that their authorizing officials had reviewed and approved the plans for five systems. Specifically, agencies provided signed letters indicating that the agencies initially approved the plans. However, agencies did not provide documentation to show that subsequent changes to the system security plan after the date of the signed letters were reviewed and approved by the authorizing official. Additionally, one agency had an expired letter. Until agencies fully address required information in their security plans, including the controls relied on by the cloud service provider, they have reduced assurance that security controls are in place and operating as intended.

Selected Agencies' Security Assessment Reports Did Not Consistently Summarize Control Effectiveness

NIST specifies that organizations document the results of security assessments in a security assessment report.⁴⁵ According to FedRAMP's guidance, agencies are to use the Control Implementation Summary to identify controls that are their responsibility and assess agency-specific controls, inclusive of any agency controls that are shared with providers.⁴⁶ The security assessment report is to summarize the control testing and describe whether the tested controls were effectively in place.

As shown in table 3, agencies did not always summarize the testing of controls on security assessment reports.

⁴⁵National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, SP-800-53, Revision 4 (Gaithersburg, MD: April 2013).

⁴⁶FedRAMP Agency Guide For FedRAMP Authorizations: *How to Functionally Reuse an Existing Authorization Version 2.0* (Washington, D.C.: Dec. 7, 2017).

Table 3: Extent to Which Selected Agencies' Security Assessment Reports (SAR) Summarized Results of Control Tests

Agency	Agency components	Selected agency system ^a	Summarized results of control tests
HHS	CDC	System 1	◐
	CMS	System 2	◐
		System 3	●
	NIH	System 4	◐
		System 5	◐
GSA	No agency component	System 6	◐
	No agency component	System 7	●
EPA	No agency component	System 8	◐
	No agency component	System 9 ^b	◐
USAID	No agency component	System 10	●

Legend:

- The security assessment report summarized testing for all selected controls.
- ◐ The security assessment report partially summarized testing of the selected controls.

HHS = Department of Health and Human Services; CDC = Centers for Disease Control and Prevention; CMS = Centers for Medicaid and Medicare Services; NIH = National Institutes of Health (CDC, CMS, and NIH are agency components of HHS); GSA = General Services Administration; EPA = Environmental Protection Agency; USAID = U.S. Agency for International Development.

Source: GAO analysis of agency documentation | GAO-20-126

Note: To determine the extent agencies tested controls, we selected 24 of the 97 core controls shown as critical to protecting a cloud service, and whether agencies summarized the testing of controls for which they were responsible. Agencies may not have responsibility for testing all 24 core controls.

^aDue to sensitivity concerns, we substituted a numeric identifier for the system names.

^bSubsequent to our review of the system's security assessment report, EPA decommissioned System 9.

The four agencies prepared security assessment reports for each of the 10 selected systems. However, agencies summarized the results of control tests for only three of the 10 systems reviewed. USAID summarized the test results in the security assessment report for the agency system we reviewed, but the other three agencies did not consistently summarize their results. For example, HHS did not

summarize test results for three controls for one system and six controls for another system. GSA did not summarize tests results for 17 controls for one of its systems. If security assessment reports do not fully summarize the test results, agencies may have limited assurance that the controls intended to protect agency data in the cloud environment are in place and operating effectively.

Selected Agencies' Remedial Action Plans Did Not Include Required Information

A remedial action plan assists agencies in identifying, assessing, prioritizing, and monitoring progress in correcting security weaknesses that are found in information systems. NIST guidelines specify that organizations develop a remedial action plan, also referred to as a plan of action and milestones, to document the organization's planned actions to correct weaknesses or deficiencies noted during the assessment of security controls of the information system.

In addition, FedRAMP guidance stated that all agencies should follow FISMA which requires agencies to have a process for documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices.⁴⁷

OMB requires that remedial action plans include the following information:

- a description of the specific weakness;
- the name of the office or organization responsible for resolving the weakness;
- an estimate of the funding required to resolve the weakness, including the anticipated source of funding;
- an estimated completion date for resolving the weakness;
- key milestones with estimated completion dates;
- any changes to the key milestones and completion dates;
- the source of the identified weakness (e.g. security assessment, program review, inspector general audit, etc.); and

⁴⁷FedRAMP Agency Guide For FedRAMP Authorizations: How to Functionally Reuse an Existing Authorization Version 2.0 (Washington, D.C.: Dec. 7, 2017).

- the status of the corrective action (ongoing, completed, etc.).⁴⁸

As shown in table 4, the four selected agencies documented remedial action plans for each of the selected systems, but did not consistently identify required information.

Table 4: Extent to Which Selected Agencies' Remedial Action Plans Included Required Information

Agency	Agency component	System remedial action plan ^a	Cited specific weakness	Identified office responsible for addressing weakness	Identified funding required, including anticipated source	Estimated completion date for resolving the weakness	Listed key milestones with completion dates	Identified changes to milestones and completion dates	Identified source of the weakness	Updated status of the corrective action
HHS	CDC	System 1	●	●	●	●	●	○	●	●
	CMS	System 2	●	●	●	●	●	●	●	●
		System 3 ^b	—	—	—	—	—	—	—	—
	NIH	System 4	●	●	●	●	○	○	●	●
		System 5	●	●	●	●	●	●	●	●
GSA	No agency component	System 6	●	●	●	●	●	●	●	●
	No agency component	System 7	●	●	●	●	●	●	●	●
EPA	No agency component	System 8	●	●	●	●	●	●	●	●
		System 9 ^c	●	●	●	●	●	●	●	●
USAID	No agency component	System 10	●	●	●	●	●	●	○	●

Legend:

- The agency included the required Office of Management and Budget (OMB) information.
- The agency partially included the required OMB information.
- The agency did not include of the required OMB information.

HHS = Department of Health and Human Services; CDC = Centers for Disease Control and Prevention; CMS = Centers for Medicaid and Medicare Services; NIH = National Institutes of Health (CDC, CMS, and NIH are agency components of HHS); GSA = General Services Administration; EPA = Environmental Protection Agency; USAID = U.S. Agency for International Development.

Source: GAO analysis of agency documentation. | GAO-20-126

^aDue to sensitivity concerns, we substituted a numeric identifier for the system names.

^bCMS did not list any open weaknesses in its remedial action plans for System 3.

^cSubsequent to our review of the system's remedial action plan, EPA decommissioned System 9.

⁴⁸Office of Management and Budget, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, M-02-01 (Washington, D.C.: Oct. 17, 2001).

As illustrated above, three plans partially identified the office responsible for addressing the weakness. Two plans did not include changes to information regarding key milestones and completion dates and two partially included the information. Further, two agencies partially identified the source of the weakness for three systems while a third agency did not identify any sources for the selected system. Until agencies include all required elements in their remedial action plans, they will be less likely to effectively assess, prioritize, and monitor efforts to resolve weaknesses in their systems.

Selected Agencies Did Not Consistently Prepare and Provide Authorization Letters to the FedRAMP PMO

OMB defines an authorization to operate as an official management decision where a federal official or officials authorize the operation of information system(s) and accept the risk to agency operations and assets, individuals, and other organizations based on the implementation of security and privacy controls. OMB requires agencies to use FedRAMP processes when granting authorizations to operate for their use of cloud services.⁴⁹

According to FedRAMP PMO guidance, authorizing officials should document the authorization of (1) the agency system supported by the cloud service and (2) the cloud service used by the agency.⁵⁰ Additionally, the agency should provide a copy of its authorization letter for the cloud service (cloud service authorization letter) to the FedRAMP program management office so that the office can verify the agency's use of the service and keep agencies informed of any changes to a provider's authorization status.

As shown in Table 5, agencies did not consistently prepare and provide the FedRAMP PMO with the cloud service authorization letter.

⁴⁹Office of Management and Budget, *Security Authorization of Information Systems in Cloud Computing Environments* (Washington, D.C.: Dec. 8, 2011).

⁵⁰FedRAMP, *Agency Guide For FedRAMP Authorizations: How to Functionally Reuse an Existing Authorization Version 2.0* (Washington, D.C.: Dec. 7, 2017).

Table 5: Selected Agencies Prepared and Provided Authorizations to the FedRAMP Program Management Office (PMO)

Agency	Agency component	Selected agency system ^a	Prepared system authorization letter	Prepared cloud service authorization letter	Provided cloud service authorization letter to the FedRAMP (PMO)
HHS	CDC	System 1	Yes	Yes	Yes
	CMS	System 2	Yes	No	No ^b
		System 3	Yes	No	No ^b
	NIH	System 4	Yes	Yes	No
		System 5	Yes	Yes	No
GSA	—	System 6	Yes	Yes	Yes
		System 7	Yes	Yes	Yes
EPA	—	System 8	Yes	No	No ^d
		System 9 ^c	Yes	No	No ^d
USAID	—	System 10	No ^e	No ^f	No

Legend: FedRAMP = Federal Risk and Authorization Management Program; HHS = Department of Health and Human Services; CDC = Centers for Disease Control and Prevention; CMS = Centers for Medicaid and Medicare Services; NIH = National Institutes of Health (CDC, CMS, and NIH are agency components of HHS); GSA = General Services Administration; EPA = Environmental Protection Agency; USAID = U.S. Agency for International Development.

Source: GAO analysis of agency documentation | GAO-20-126

^aDue to sensitivity concerns, we substituted a numeric identifier for the system names.

^bAlthough CMS sent a system authorization letter to the FedRAMP PMO, the letter did not clearly reflect authorization of a cloud service.

^cSubsequent to our review of the system's authorization letter, EPA decommissioned System 9.

^dAccording to the FedRAMP PMO official, EPA did not submit copies of its cloud service authorization letters for Systems 8 and 9.

^eWhile USAID had a current extension memo, the memo did not cover the period of system operation after the authorization letter had expired.

^fWhile USAID did not issue a separate cloud service authorization letter for the cloud service; the agency documented a risk decision memo and authorized their use of a cloud service without an internal agency authorization to operate letter.

GSA prepared both system and cloud service authorization letters for its two selected systems. However, the other three agencies did not consistently prepare the letters. Specifically, USAID did not consistently prepare letters authorizing the cloud service and the system supported by the cloud service. In addition, HHS and EPA did not consistently prepare letters authorizing their use of the cloud services. Further, EPA, HHS, and USAID did not consistently provide the FedRAMP PMO with authorization letters for cloud services.

Although GSA and an HHS component, CDC, provided cloud service authorization letters to the FedRAMP PMO, only HHS included the

requirement to provide the letter to the FedRAMP PMO in its guidance. Three of the four selected agencies did not include this requirement in their guidance. Not including this requirement in their security guidance could be a potential reason for agencies' inconsistent implementation. If agencies do not provide copies of their cloud service authorization letters to the program management office, the office may not have accurate information on which agencies are using approved cloud services. Further, the lack of such information could result in the office being delayed in notifying agencies when a service provider's authorization has been revoked or a provider has experienced a security incident.

Agencies provided various reasons for not including required information in FedRAMP authorization documents. Such reasons included the agency was restricted from documenting proprietary information concerning the cloud service provider's portion of the shared control in the security plan and the agency was tracking all remedial actions, but the agency did not include them in the plan it provided to us. By not including the required information, agencies have reduced assurance that controls over cloud services have been effectively implemented.

Program Participants Reported Improved Security and other Benefits, but also Identified Challenges

FedRAMP participants identified a number of the program's benefits, such as improved security of agencies' data and increased efficiency for providers to obtain authorizations. Participants also cited a number of challenges, such as the agency resources needed for authorizing a cloud service or the resources needed by the provider to implement the program's requirements. To address challenges, GSA has taken steps to improve the program, but its guidance on FedRAMP's requirements and participant's responsibilities was not always clear and the program's process for monitoring the status of security controls over cloud services was limited.

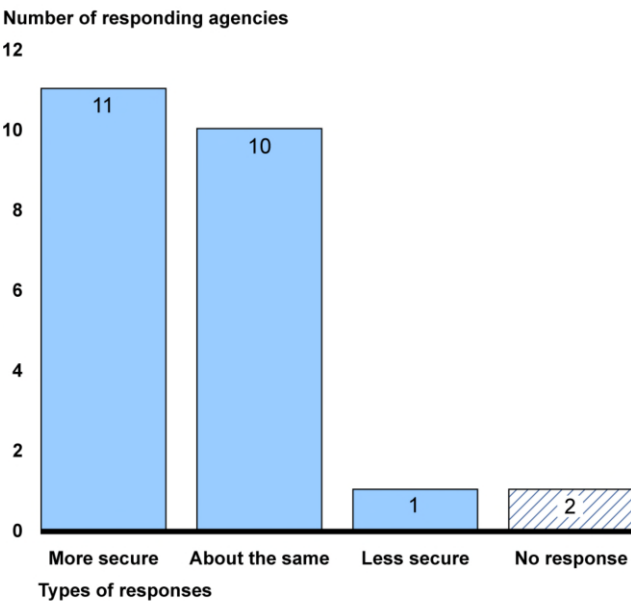
Participants Identified the Benefits of the Program

Most of the Surveyed Agencies Reported that FedRAMP Generally Improved or Maintained the Same Security of Their Data

One of the intended benefits of FedRAMP is to provide enhanced security over cloud services. In responding to our survey, almost half of the agencies reported that FedRAMP had generally improved the security of their data. Specifically, as shown in figure 3, 11 agencies responded that FedRAMP had made their data more secure and 10 agencies responded

that FedRAMP had maintained the same level of security as before the data were moved into a FedRAMP-authorized cloud environment.⁵¹

Figure 3: Surveyed Agencies' Responses on Whether FedRAMP Made Their Data in Cloud Environments More or Less Secure



Source: GAO analysis based on responses to GAO's agency survey. | GAO-20-126

Note: The 24 Chief Financial Officers Act agencies that responded to our survey 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 United States Agency for International Development. Two agencies skipped this question of the survey.

However, one agency reported that FedRAMP had made the agency's data less secure. According to the agency, the FedRAMP authorization process did not ensure that the data were more secure because the amount of control and insight the agency had over its data after moving to the cloud was reduced. The agency indicated that this loss of control and

⁵¹Two agencies did not respond to this question. Agencies did not explain whether their responses were based on a specific type of authorization (agency or JAB) or cloud service model (Software as a Service, Platform as a Service, and Infrastructure as a Service).

insight could pose risks with implementing controls, such as controls for data encryption.

Agencies also cited other security-related difficulties with FedRAMP. To illustrate, 19 of 23 agencies reported that it was difficult for their cloud service providers to implement trusted internet connections (TIC) requirements with their cloud services. Federal agencies are required to implement TIC, which establishes a set of baseline security capabilities for external network connections, such as connections to cloud environments. Because of this requirement, an agency official stated that the implementation of TIC may not be supported by all FedRAMP authorized cloud service providers. According to the Director of FedRAMP, agencies should work with cloud service providers to ensure TIC compliance.

JAB technical representatives stated that because federal agencies are required to be TIC compliant, there was a need to develop guidance to address this issue. Additionally, JAB technical representatives stated the program needed to have a better integrated approach to identifying cybersecurity risks and the extent to which those risks are mitigated within the cloud. In its June 2019 *Federal Cloud Computing Strategy*, OMB mentioned that DHS was working with agencies on agency-specific approaches to address TIC requirements in new operational environments, such as cloud services. Subsequently, OMB issued a memorandum on September 12, 2019 that updated its guidance on the TIC initiative. The memorandum is intended to enhance agencies' TIC implementation by providing them with increased flexibilities to use modern security capabilities and establishing a process to respond to advancements in technology and rapidly evolving threats. This memorandum rescinded OMB's prior TIC guidance as part of the office's efforts to reduce reporting burden.⁵²

In addition to challenges with implementing TIC, agencies cited other security-related challenges. These challenges pertained to, for example, cloud service providers not being able to comply with NIST's FIPS 140-2 encryption requirements as well as requirements for multifactor

⁵²Office of Management and Budget, *Update to the Trusted Internet Connections (TIC) Initiative*, M-19-26 (Washington D.C.: Sept. 12, 2019).

Agencies Cited the Use of
Third-Party Assessors and JAB
Authorizations as Beneficial for
Authorizing Cloud Services

authentication.⁵³ According to the Director of FedRAMP, FIPS 140-2 and multifactor authentication are requirements included within the FedRAMP moderate and high baselines.

In their survey responses, federal agencies identified several program elements as being very beneficial to authorizing cloud services through FedRAMP as shown in figure 4.

⁵³National Institute of Standards and Technology, *Security Requirements for Cryptographic Modules*, Federal Information Processing Standard 140-2, (Gaithersburg, MD: May 2001).

Figure 4: Responding Federal Agencies' List of Beneficial Federal Risk and Authorization Management Program (FedRAMP) Elements

FedRAMP elements

Value of 3PAO's assessments



Reduction in costs by using FedRAMP JAB authorizations



FedRAMP guidance and education resources



Reduction of efforts to assess and authorize cloud services



Reduction in costs by using FedRAMP agency authorizations



Support from the FedRAMP PMO



Support for risk-based security management



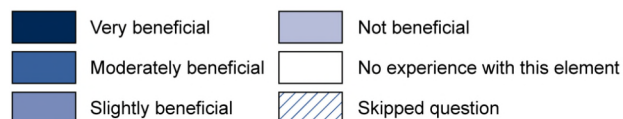
Consistency of JAB officials' review of authorization packages



0 4 8 12 16 20 24

Number of responding agencies

3PAO (Third-party assessment organization), JAB (Joint Authorization Board), PMO (Program Management Office)



Source: GAO analysis based on responses to GAO's agency survey. | GAO-20-126

Note: The 24 Chief Financial Officers Act agencies that responded to our survey 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; and Social Security Administration, and the United States Agency for International Development.

These FedRAMP elements are listed in the order of the elements receiving the highest combined total of very, moderately, and slightly beneficial responses.

"Consistency" means the review of the authorization packages by the agency and JAB officials' are exactly the same as the FedRAMP program requirements.⁵⁴

Agencies identified third-party independent assessments and JAB authorizations as the top two benefits of the program.

- **Third-party assessment organizations provided independent assurance.**⁵⁵ According to agencies, FedRAMP's use of third parties for assessing controls helped to provide assurance of the cloud service provider's security posture. Twenty-two of 23 agencies indicated that FedRAMP's use of third-party assessments of cloud services was generally beneficial⁵⁶ to authorizing cloud services. Specifically, 10 agencies found the assessments to be very beneficial, while 11 found them to be moderately beneficial, and one agency found them to be slightly beneficial. One agency did not have experience with the assessments and the other agency skipped the question.

According to agency officials, the work conducted by trusted third-party assessors helped ease the agencies' review of the service and avoid duplication of efforts. This better enabled the agencies to leverage services that had been assessed and validated as meeting the program's security control requirements. In addition, agency officials stated that the validated services provided their agencies with assurances of the security of the cloud services that in turn, allowed them to reduce the time needed to authorize the service.

JAB authorizations reduced efforts for reviewing packages. Twenty-one of 23 agencies reported that it was generally beneficial to leverage JAB authorizations since doing so reduced costs in reviewing CSP

⁵⁴For questions where we asked about benefits associated with participation in FedRAMP, we used a 5-point scale to measure the extent of benefit: very beneficial, moderately beneficial, slightly beneficial, not beneficial, and no experience with this element. For the purposes of this report, we combined the responses for very beneficial, moderately beneficial, and slightly beneficial to total the number of the 23 CFO Act agencies responding.

⁵⁵Third-party assessment organizations (3PAO) are FedRAMP accredited independent assessment organizations that verify cloud service providers' security implementations and provide the overall risk posture of a cloud environment for a security authorization decision.

⁵⁶Beneficial includes survey responses of very, moderately, and slightly beneficial.

assessment and authorization packages. Further, 21 agencies cited that leveraging JAB authorizations also reduced their time and efforts. The reduction in the costs associated with reviewing CSP assessment and authorization packages was one of the responding agencies' most frequently identified potential benefits of the program. Specifically, 10 agencies found this aspect of the program to be very beneficial, eight agencies found it to be moderately beneficial, and three agencies found it to be slightly beneficial. One agency skipped this question.

Cloud Service Providers Cited
Program Guidance and
Standard Security
Requirements as Beneficial to
Implementing FedRAMP

Cloud service providers identified a number of FedRAMP elements as being very beneficial to implementing the program. As shown in figure 5, cloud service providers identified the availability of FedRAMP guidance and its standard security requirements as the top two benefits to implementing the program's requirements.⁵⁷

⁵⁷For questions where we asked about benefits associated with participation in FedRAMP, we used a 5-point scale to measure the extent of benefit: very beneficial, moderately beneficial, slightly beneficial, not beneficial, and no experience with this element. For the purposes of this report, these FedRAMP elements are listed in the order of the elements receiving the highest combined total of very, moderately, and slightly beneficial responses.

Figure 5: Surveyed Cloud Service Providers (CSP) List of Beneficial Federal Risk and Authorization Management Program (FedRAMP) Elements

FedRAMP elements

FedRAMP guidance and education resources



Standard security requirements available for all CSPs



Support from the FedRAMP Program Management Office (PMO)



Consistency of agency officials' review of authorization packages



Consistency of JAB officials' review of authorization packages



0 7 14 21 28 35 42 49

Number of responding cloud service providers

JAB (Joint Authorization Board)



Source: GAO analysis based on responses to GAO's cloud service provider survey. | GAO-20-126

Note: Consistency means whether the review of the authorization packages by the agency and JAB officials' are exactly the same as the FedRAMP program requirements.

Specifically, 19 of 47 cloud service providers that responded to the survey reported that the availability of clear guidance and education resources was very beneficial in implementing the program's requirements. In addition, 18 cloud service providers cited FedRAMP's use of standard security requirements, and 16 reported support from the program management office as very beneficial.

Participants Identified Various Challenges with Implementing FedRAMP

FedRAMP participants indicated that implementing certain elements of the program were challenging. Participants specifically identified the authorization process, remedial actions, and time and resources as key challenges.

Authorization process and requirements.

- **Complex authorization process.** Surveyed participants—agencies and cloud service providers—responded that simplifying the agency authorization process would help them to better understand and manage their ongoing authorizations and continuous monitoring efforts. For example, 17 of 23 agencies, responding to this question, identified the agency authorization process as an area for improvement as did 30 of 47 surveyed cloud service providers. Survey respondents indicated that the agency authorization process should be streamlined to be less-restrictive and time-consuming. Agencies also reported that overcoming the complexity of the authorization process was one of their largest hurdles. According to the Director of FedRAMP, the FedRAMP PMO encourages agencies to streamline their agency authorization processes to be less-restrictive and time-consuming.
- **Limitations with reviewing authorization packages.** Agencies also identified reviewing authorization packages as a challenge. Agencies reported in the survey and during interviews that there were limitations in their ability to review cloud security packages prior to selecting a cloud service provider. Agencies that are currently using or want to evaluate specific FedRAMP authorized cloud services are able to access FedRAMP security packages directly through the FedRAMP Secure Repository, located on OMB MAX portal.⁵⁸ However, agencies are given a 30-day period to access packages, which one agency official stated is too short of a time period for them to properly review documentation. Although access is limited to 30 days, agencies are able to renew the access by sending an email to the FedRAMP program management office. The Director of FedRAMP indicated that agencies can work directly with cloud service providers to obtain additional permissions to the package to save, print, email, post, publish, or reproduce.

⁵⁸OMB MAX portal is a secure repository that supports low and moderate impact levels' security packages.

In addition, agencies expressed challenges with restrictions on downloading the packages, which limited their ability to automate their review of packages and subsequent monitoring of changes to the services security posture. Agencies also cited challenges with sharing review-related information due to the restrictive nature of cloud service nondisclosure agreements. The Director of FedRAMP mentioned that agencies can work directly with cloud service providers to obtain additional access permissions to their packages.

- **Lack of uniform guidance for selecting cloud services.** Federal agencies suggested that uniform guidance on authorization packages could assist FedRAMP customers in making better risk-based decisions in selecting cloud services. Agency officials we interviewed stated the quality and reviews of authorization packages approved through FedRAMP varied. Officials stated that inconsistencies in both FedRAMP agency and JAB provisional authorization packages have required some agencies to perform additional work. According to the officials, while the JAB process takes longer, the review appears to be more detailed than the agency process. Officials noted that improving guidance on reviewing authorization packages could help with the consistency and quality of the agency package reviews. The FedRAMP PMO has taken action and published guidance during our engagement to address more details of the authorization process. In addition, according to the Director of FedRAMP, the FedRAMP PMO launched a series of training events between February 2018 and June 2019 that provided detailed guidance into the package review process.
- **Need for improved collaboration and coordination.** Participants also identified opportunities for improving collaboration and coordination. Federal agencies suggested that improved collaboration among federal agencies in leveraging cloud services could provide transparency on the cloud service providers and the services other agencies are using. This could inform agencies on whether those services could be adopted to fit the need of their missions.

Agencies also mentioned that FedRAMP PMO could improve its coordination across federal agencies and cloud service providers to provide consistent information and help facilitate opportunities to improve the program. For example, three participants suggested improving cross-agency collaborations for cloud authorizations. Additionally, one survey participant noted that improved collaboration within the cloud service provider community could provide a better understanding of the impacts and associated cost of potential changes to program's policies or requirements before they are made.

According to officials from the FedRAMP PMO, their standard practice is to solicit feedback from industry and agency stakeholders prior to release of significant guidance. They added that they plan to continue collaborating with agency and industry partners.

Remedial action process. In responding to our survey, 9 of 23 agencies reported that the lack of clarity on actions taken to resolve weaknesses in systems supporting cloud services was a major or moderate challenge. Specifically, two agencies cited this area as a major challenge and seven as a moderate challenge. Two agencies suggested that the program management office could make improvements by providing better visibility and traceability of the remedial action process to inform agencies on the risks associated with a cloud service.

Participants responded that the remedial action process could be improved by having structured procedures for aggregating system vulnerabilities and deficiencies. This would provide agencies with better information on weaknesses identified by cloud service providers or their third party assessors in order to better consider risks prior to the purchase or use of cloud services. Additionally, agencies cited the need for improvements to the consistency of remedial action plans. Specifically, agencies cited the need for a consistent format and content of remedial action plans among security packages. Further, one cloud service provider stated that outcome-based performance metrics were a better measure of monitoring the status and effectiveness of the ongoing authorization and assessment of cloud services, as opposed to only relying on remedial action plans.

According to the Director for FedRAMP, the FedRAMP PMO developed additional remedial action guidance in February 2018 and a dedicated webpage specific to the remedial action process in January of 2018. Additionally, the Director noted that for all JAB provisional authorizations, the FedRAMP PMO and JAB analyzes raw data on vulnerability scans and provides a one-page summary report that is available to agencies within the OMB MAX portal.

Commitment of time and resources to complete and maintain an agency authorization. The amount of time to complete an agency authorization to operate for a cloud service was cited as one of the most challenging aspects of FedRAMP. In responding to our survey, six agencies cited the commitment of time and resources for agency authorizations as a major challenge; five agencies identified it as a moderate challenge; and six as a minor challenge.

One responding agency mentioned that the time and costs associated with completing and maintaining an ongoing agency authorization was burdensome to both the agency and cloud vendor. This burden was due to a lack of allocated agency resources to continue implementing the program's requirements. In response to this challenge, the program management office has streamlined the authorization process for low-risk systems to allow for risk-based decisions that can reduce the time and resources required for an agency authorization.

In addition, 36 of 47 cloud service providers responding to our survey indicated that the significant amount of resources required to implement the program's requirements for an authorization was a major or moderate challenge.

Additionally, JAB technical representatives identified many of the challenges and opportunities for improving the program that agencies and cloud service providers identified. In addition, the officials stated that the FedRAMP PMO is aware of these issues and has taken steps to address them. According to the JAB technical representatives, the FedRAMP PMO's program intended improvements include, but are not limited to, updates to guidance and education resources, plans to automate the continuous monitoring process with vulnerability scanning tools, and reduced time and costs associated for completing the authorization process for both customer agencies and cloud service providers.

According to the Director for FedRAMP, the FedRAMP PMO has continued to make enhancements based on industry and agency feedback. The official reported that numerous guidance documents, relating to continuous monitoring, the agency authorization process, and FedRAMP designations have been released during our engagement. The official also mentioned that the PMO actively seeks feedback from stakeholders and that additional opportunities for FedRAMP training was available.

GSA Took Steps to Improve FedRAMP, but Program Guidance Was Not Always Clear and the Process for Monitoring Security Controls Was Limited

GSA has taken a number of steps to improve FedRAMP. Among other things, the office has provided updated instructions for completing authorization packages and established and updated its training portal to help agencies and cloud service providers better understand the steps required for obtaining an authorization. In addition, the office has taken steps to streamline the authorization process and provided additional guidance on continuous monitoring of security controls over cloud services.

Nevertheless, FedRAMP's requirements and guidance on implementing controls were not always clear and the program's process for monitoring the status of security controls over cloud services was limited.

Clarity in program requirements and responsibilities. Agencies reported challenges with understanding FedRAMP's requirements and the process for granting an agency authorization. Specifically, agencies cited the need for clearer guidance on requirements and agency responsibilities for completing and maintaining an authorization. Eight agencies reported the clarity of FedRAMP requirements associated with the agency authorization process as a moderate challenge; whereas nine identified it as a minor challenge and no agencies reported it as a major challenge. Five agencies reported this was not a challenge.

In addition, 20 of 24 surveyed agencies indicated that additional guidance describing roles and responsibilities would be very or moderately useful to their participation in FedRAMP. Further, 37 of 47 cloud service providers specified that additional guidance for describing the security roles and responsibilities between agencies and cloud service providers was needed. Both agencies and cloud service providers commented that existing guidance for using the program does not fully address control implementation roles and responsibilities and that a process should be established to address these issues.

Officials from selected agencies also indicated that responsibilities were not always clearly detailed. Specifically, HHS, GSA, and USAID officials stated that guidance for using FedRAMP could be clearer on helping define roles and responsibilities between agencies and providers in implementing security controls for cloud services. The JAB technical representatives we interviewed acknowledged that while control implementation responsibilities between the agency and cloud service provider are defined in the Control Implementation Summary, in some cases, shared responsibilities are not clearly delineated. The JAB technical representatives stated that the unclear shared responsibilities

could lead to inconsistent implementation of certain controls between the agency and its provider. According to the Director of FedRAMP, it is the cloud service providers' responsibility to ensure the spreadsheet identifying control responsibilities are completed accurately and consistently.

Our analysis of agency documentation of required information in authorization packages found that the cause of selected agencies' gaps in required information for security plans, security assessment reports and remedial action plans were due in part, to unclear guidance for implementing their control responsibilities. If responsibilities are not clear, agencies may have reduced ability to ensure that controls over the cloud services they authorized are in place and effective.

Limited capabilities for continuously monitoring security controls.

FedRAMP's continuous monitoring process does not allow for an automated review of control requirements by agencies with security management tools. According to NIST SP 800-137, security continuous monitoring is maintaining an ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.⁵⁹ In addition, NIST mentions that timely, relevant, and accurate information is vital, particularly when resources are limited and agencies must prioritize their efforts. According to the program's officials, they will be working with NIST to incorporate automation into the authorization process.

Based on our work and survey responses from agencies and cloud service providers, a number of weaknesses with the program's continuous monitoring process existed. For example, copy-protected PDFs, Word documents, and Excel spreadsheets comprised the remedial action plans and other documents supporting continuous monitoring of FedRAMP cloud service provider controls. Because of the static nature of the documents, including restrictions on copying information concerning cloud service provider controls, the documents could not be readily integrated with agencies' automated security management tools in providing ongoing awareness of control implementation. Further, agency staff would have to spend time manually accessing and reviewing the documents each time they needed to determine the status of a cloud

⁵⁹National Institute of Standards and Technology, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, SP-800-137, (Gaithersburg, MD: September 2011).

service's implementation of a particular control. Agency personnel would also have to confirm that the documents they reviewed were the most current version. According to the Director of FedRAMP, agencies may request unrestricted access to the security package directly from the provider.

Agencies' survey responses also indicated that: 1) remedial action plans, used in continuous monitoring, were not updated consistently, 2) the manual process did not allow for automated data feeds into their continuous monitoring tools, and 3) restrictions on copying documents reduced information sharing within the agency. Further, 21 of 23 agencies responded that FedRAMP's continuous monitoring of cloud security controls was a needed area of improvement.

Cloud service providers also reported difficulties (36 of 47) with implementing continuous monitoring which could highlight the need for further improvements. In response, the Director of FedRAMP indicated that as of October 30, 2018, the FedRAMP PMO consolidated all continuous monitoring guidance documents, templates, and blog posts to a single webpage for ease of access by program stakeholders.

JAB technical representatives also acknowledged challenges with implementing continuous monitoring such as difficulties with using continuous monitoring reports to assess the security posture of a cloud service. According to JAB technical representatives, agencies are responsible for reviewing continuous monitoring reports from the cloud service providers, but not all agencies could effectively conduct continuous monitoring. For example, an agency's continuous monitoring efforts could be affected from not receiving a timely notification that its cloud service provider has uploaded the required monthly continuous monitoring updates, including updates to remedial actions.

According to the Director of FedRAMP, the OMB MAX portal⁶⁰ provides the capability for agencies to receive automatic notifications when there is

⁶⁰Cloud service providers do not always store their FedRAMP authorization packages in the OMB MAX portal. For packages rated as high-risk impact level, cloud service providers store packages in their own virtual reading rooms, where access and monitoring procedures may differ than those for OMB MAX. According to FedRAMP's PMO, the program office works with the cloud service providers to ensure the confidentiality and integrity of all authorization packages regardless of their risk levels. The PMO stated that, in the future, it may host an environment for the systems that are consider high impact, but currently doing so is cost prohibitive.

an update to the continuous monitoring. Agencies can enable updates by selecting the “Watch this Page” option in the menu bar. While the FedRAMP PMO recommends agencies to enable this feature, agencies were not aware of the feature. As a result, agencies may not be aware that such updates have taken place and tend to be reliant on a providers’ ability to ensure that effective security practices are in place. The JAB technical representatives commented that as cloud services evolve and mature, the continuous monitoring process needs to become more automated and user-friendly to provide real-time awareness of the security status of cloud services.

Until the PMO allows for more options to automate continuous monitoring, agencies may have less assurance that they will receive timely information on the extent that controls are being effectively implemented for the cloud services they are using. In addition, as more federal agencies move toward DHS’s Continuous Diagnostics and Mitigation program, automation may become even more important.⁶¹

Conclusions

Although federal agencies increased their use of FedRAMP, they continued to authorize the use of cloud services that had not been approved through the program. While OMB requires agencies to use FedRAMP to authorize the use of cloud services, it did not monitor or ensure that agencies used the program to authorize cloud services. As a result, agencies have less assurance that security controls over cloud services have been consistently implemented.

The selected agencies did not fully address key elements necessary for implementing the FedRAMP authorization process. Agencies did not consistently address required information for implementing controls, summarizing control tests, and tracking corrective actions. In addition, agencies also did not always provide the FedRAMP PMO with their cloud service authorization letters. By not fully addressing these elements, agencies have less assurance that they have effectively implemented security controls intended to protect their data in cloud environments and that those controls operating as intended.

⁶¹The Department of Homeland Security’s Continuous Diagnostics and Mitigation Program is intended to provide federal departments and agencies with commercial off-the-shelf capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first.

FedRAMP participants identified a number of benefits as well as challenges with the program. Among other benefits, several agencies indicated that FedRAMP improved the security of their data. However, participants identified challenges with the program and areas where the program could be improved. GSA has taken a number of actions toward improving and furthering the program's progress, nonetheless unclear guidance and limitations with FedRAMP's continuous monitoring process could hamper the program's effectiveness and result in agencies implementing the program unevenly.

Recommendations for Executive Action

We are making a total of 25 recommendations—1 recommendation to OMB and 24 recommendations to the 4 selected agencies in our review, including additional recommendations to GSA as the FedRAMP program lead.

The Director of OMB should establish a process for monitoring and holding agencies accountable for authorizing cloud services through FedRAMP. (Recommendation 1)

The Administrator of GSA should direct the Director of FedRAMP to clarify guidance to agencies and cloud service providers on program requirements and responsibilities. (Recommendation 2)

The Administrator of GSA should direct the Director of FedRAMP to improve the program's continuous monitoring process by allowing more automated capabilities, including for agencies to review documentation. (Recommendation 3)

The Administrator of GSA should update security plans for selected systems to include the description of security controls and reviews and approvals plan. (Recommendation 4)

The Administrator of GSA should update the security assessment report for the selected system to identify the summarized results of control effectiveness tests. (Recommendation 5)

The Administrator of GSA should update the list of corrective actions for selected systems to identify the responsible office and estimated funding required and anticipated source of funding. (Recommendation 6)

The Administrator of GSA should develop guidance requiring that cloud service authorization letters be provided to the FedRAMP program management office. (Recommendation 7)

The Secretary of HHS should direct the Director of CDC to update the security plan for the selected system to identify the authorization boundary, the system operational environment and connections, a description of security controls, and the individual reviewing and approving the plan and date of approval. (Recommendation 8)

The Secretary of HHS should direct the Director of CDC to update the security assessment report for the selected system to identify the summarized results of control effectiveness tests. (Recommendation 9)

The Secretary of HHS should direct the Director of CDC to update the list of corrective actions for the selected system to identify the specific weaknesses, funding source, changes to milestones and completion dates, identified source of weaknesses, and status of corrective actions. (Recommendation 10)

The Secretary of HHS should direct the Administrator of CMS to update the system security plans for selected systems to identify a description of security controls. (Recommendation 11)

The Secretary of HHS should direct the Administrator of CMS to update the security assessment report for selected system to identify the summarized results of control effectiveness tests. (Recommendation 12)

The Secretary of HHS should direct the Administrator of CMS to update and document the CMS remedial action plan for the selected system to identify the anticipated source of funding. (Recommendation 13)

The Secretary of HHS should direct the Administrator of CMS to prepare letters authorizing the use of cloud services for the selected systems and submit the letters to the FedRAMP program management office. (Recommendation 14)

The Secretary of HHS should direct the Director of NIH to update security plans for selected systems to identify the authorization boundary, system operation in terms of mission and business processes, operational environment and connections, and a description of security controls. (Recommendation 15)

The Secretary of HHS should direct the Director of NIH to update the security assessment report for selected systems to identify summarized results of control effectiveness tests. (Recommendation 16)

The Secretary of HHS should direct the Director of NIH to update the NIH list of corrective actions for selected systems to identify estimated funding and anticipated source of funding, key milestones with completion dates, and changes to milestones and completion dates. (Recommendation 17)

The Secretary of HHS should direct the Director of NIH to submit the division's letters authorizing the use of cloud services for the selected systems to the FedRAMP program management office. (Recommendation 18)

The Administrator of EPA should update security plan for the selected operational system to identify a description of security controls, and the individual reviewing and approving the plan and date of approval. (Recommendation 19)

The Administrator of EPA should update the security assessment report for the selected operational system to identify the summarized results of control effectiveness tests. (Recommendation 20)

The Administrator of EPA should update the list of corrective actions for the selected operational system to identify the specific weakness, estimated funding and anticipated source of funding, key remediation milestones with completion dates, changes to milestones and completion dates, and source of the weaknesses. (Recommendation 21)

The Administrator of EPA should prepare the letter authorizing the use of cloud service for the selected operational system and submit the letter to the FedRAMP program management office. (Recommendation 22)

The Administrator of EPA should develop guidance requiring that cloud service authorization letter be provided to the FedRAMP program management office. (Recommendation 23)

The Administrator of USAID should update the list of corrective actions for the selected system to include the party responsible for addressing the weakness, and source of the weakness. (Recommendation 24)

The Administrator of USAID should prepare the letter authorizing the use of cloud service for the selected system and submit the letter to the FedRAMP program management office. (Recommendation 25)

Agency Comments and Our Evaluation

We provided a draft of this report to OMB and the 24 CFO Act agencies for review and comment. In response, we received comments from OMB and the four agencies (GSA, HHS, EPA, and USAID) to which we made recommendations.

Specifically, in comments provided via email on October 15, 2019, an OMB Associate General Counsel stated that OMB neither agreed nor disagreed with our draft recommendation that it establish a process for monitoring and enforcing agency compliance with its guidance on using FedRAMP. The official asserted that OMB does not have a mechanism for enforcing agencies' compliance with its guidance on FedRAMP.

However, we believe OMB can and should hold agencies accountable for complying with its policies. Policies without accountability mechanisms present the risk that the benefits expected from their implementation will likely not be realized. To ensure our position is clearly stated, we modified the recommendation to state that OMB should establish a process for monitoring and holding agencies accountable for authorizing cloud services through FedRAMP.

In addition, the OMB Associate General Counsel stated that the report did not appropriately reflect FedRAMP's progress. We disagree. Although identifying the program's progress was not one of our objectives, we highlighted several areas throughout the report where progress was achieved such as the agencies' increasing use of the program to authorize cloud services and the development of additional guidance and training opportunities for using the program.

The OMB Associate General Counsel also commented on the duration of the audit. Additionally, OMB commented that our use of surveys on agencies and cloud service providers' use of FedRAMP did not address whether the program was meeting its overall objectives, but presented more of a perception. As discussed in the scope and methodology for this review, and consistent with our objectives, the purpose of the surveys was to obtain program participants' views on the benefits, challenges, and their use of the program. Additionally, our review, as designed, including our timelines, allowed us the opportunity to best assess the implementation of the program. OMB also provided technical comments, which we have incorporated into our report as appropriate.

In its written comments, GSA concurred with each of our six recommendations. The agency stated that it is developing a plan to address the recommendations. GSA's comments are reprinted in appendix IV.

In written comments, HHS concurred with each of our 11 recommendations. One operating division, CDC, noted that our observations were narrowly focused on authorization artifacts and did not take their FISMA compliant authorization process into account. We disagree. Our reviews of their FedRAMP authorization processes included procedures for reviewing security practices that are required under FISMA. The department stated that it would work with its operating divisions to address our recommendations. HHS's comments are reprinted in appendix V. The agency also provided technical comments, which we incorporated into the report as appropriate.

EPA provided written comments, in which it disagreed with the findings for two recommendations, partially agreed with the findings for one recommendation and disagreed with two other recommendations.

- EPA disagreed with the finding supporting our recommendation to update the security plans for the two selected systems to identify specific required information. The agency stated that one of the systems we selected for review was no longer in production and not used for EPA's operations. Nevertheless, the agency stated that its chief information security officer would coordinate with the agency's information security officers to ensure that security plans for the systems used to support its operations include all required information.

We acknowledged in the report that EPA discontinued the system after we completed our review of the system's authorization package. However, our recommendation in the draft report did not clearly convey that it was intended only for the operational system. Thus, we revised the recommendation to specify the system in operation.

- EPA disagreed with the finding supporting our recommendation to update the security control assessment report for one of the selected systems to identify the summarized results of control effectiveness tests. The agency stated that it used a FedRAMP certified third-party assessor that provided full documentation of control test results.

However, neither the security assessment report nor other documents that EPA provided to us summarized information on how the agency tested the effectiveness of its corrective actions to rectify a critical control that had previously failed. As a result, EPA had limited assurance that it had effectively implemented a control that was intended to protect agency data in the cloud environment. Accordingly, we believe that our recommendation is warranted.

- EPA partially agreed with the finding supporting our recommendation to update the list of corrective actions for the selected systems to

identify specific required information. The agency stated that one of the systems we selected for review was no longer in production and not used for EPA's operations. In addition, the agency said that the Chief Information Security Officer would coordinate with agency information security officers to ensure that plans of corrective actions and milestones include all required information, as appropriate.

We acknowledged in the report that EPA discontinued its use of the system after we completed our review of the system's authorization package. However, our recommendation in the draft report did not clearly convey that it was intended only for the operational system. As a result, we revised the recommendation to specify the system in operation.

- EPA disagreed with our recommendation that the agency prepare letters authorizing the cloud services for the selected systems and submit the letters to the FedRAMP program management office. The agency stated that one of the systems we selected for review was no longer in production and not used for EPA's operations. We acknowledged in the report that EPA had discontinued the system after we completed our review of the system's authorization package. However, our recommendation in the draft report did not clearly convey that it was intended only for the operational system. We have revised the recommendation accordingly.

EPA also stated that it prepares and sends authorization letters for cloud services to the FedRAMP PMO. However, at the time of our review, the FedRAMP PMO stated it had not received the cloud service authorization letter from EPA for the selected operational system. We believe that our revised recommendation for EPA to prepare and send the cloud service authorization to the FedRAMP PMO for the operational system is warranted.

- EPA disagreed with our recommendation that the agency develop guidance requiring cloud service authorization letters to be provided to the FedRAMP program management office. The agency stated that it had a standard operating procedure in which the EPA Chief Information Security Officer forwards the letters to the FedRAMP program management office. However, the agency did not provide us a copy of the standard operating procedure or otherwise demonstrate that it had such an operating procedure. Thus, we continue to believe that the recommendation is warranted.

EPA's comments are reprinted in appendix VI. The agency also provided technical comments, which we incorporated into the report, as appropriate.

Further, in written comments, USAID concurred with two of our three recommendations, but did not concur with the third. Specifically, USAID concurred with the two recommendations for the agency to update the list of corrective actions for the selected system and prepare the letter authorizing the use of cloud services supporting the system and submit it to the FedRAMP program management office.

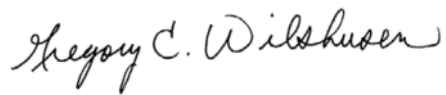
However, USAID did not concur with our recommendation to update the system security plan for the selected system to identify the authorization boundary, system operational environment and connections, and a description of security controls. The agency provided additional information that it had documented the authorization boundary, system operational environment and connections, and security controls for the selected system. Upon our review of the information, we agreed that the agency had sufficiently documented these items. Accordingly, we revised our report to reflect the agency's actions and withdrew the recommendation from the report. USAID's comments are reprinted in appendix VII.

In addition to the aforementioned responses, two agencies—the Department of Veterans Affairs and the Social Security Administration—provided written responses stating that they had no comments on the draft report. These agencies' responses are reprinted in appendixes VIII and IX, respectively. Also, the Department of Justice provided technical comments, which we incorporated into the report as appropriate.

Sixteen CFO agencies provided emails stating that they had no comments on the draft report. These agencies were the Departments of Agriculture, Commerce, Defense, Education, Energy, Homeland Security, Housing and Urban Development, the Interior, Labor, State, Transportation, and the Treasury; as well as the National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, and Office of Personnel Management. We did not receive a response from one agency—the Small Business Administration.

We are sending copies of this report to appropriate congressional committees, the Director of the Office of Management and Budget, the 24 CFO Act agencies; and other interested parties. This report will also be available at no charge on our website at <http://www.gao.gov>.

If you or your staff have any questions on matters discussed in this report, please contact Gregory C. Wilshusen at (202) 512-6244 or WilshusenG@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 X.



Gregory C. Wilshusen
Director, Information Security Issues

List of Congressional Requesters

The Honorable Ron Johnson
Chairman
The Honorable Gary Peters
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Thomas Carper
Ranking Member
Permanent Subcommittee on Investigations
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Susan M. Collins
United States Senate

The Honorable Jim Jordan
Ranking Member
Committee on Oversight and Reform
House of Representatives

Appendix I: Objectives, Scope, and Methodology

Our objectives were to determine the extent to which 1) federal agencies used FedRAMP to authorize the use of cloud services, 2) selected agencies addressed key elements of the program's authorization process, and 3) program participants identified FedRAMP benefits and challenges. The scope of our review included the 24 agencies covered by the *Chief Financial Officers Act*.¹

To address the three objectives, we developed one survey for the 24 agencies and another survey for 83 cloud service providers identified by the FedRAMP Program Management Office (PMO) as participating in the program. We administered these web-based surveys between April and November 2018. We sent two follow-up email messages to all nonrespondents and subsequently attempted to contact the remaining nonrespondents by telephone or email at least twice more.

To inform our survey questions and options, we designed our questionnaire based on FedRAMP PMO documentation and interviews with the 24 agencies and cloud service providers. We pretested the surveys with three major federal agencies, three cloud service providers, and one internal GAO group. We requested that agency chief information officers and chief information security officers review and confirm the results of the survey. We received completed surveys from 24 of 24 agencies (a 100 percent response rate) for our agency survey and 47 of the 83 cloud service providers identified (a 57 percent response rate) for our cloud service provider survey. Not all survey respondents provided answers to all survey questions.

With any survey, error can be introduced with respect to measurement of concepts, representation of respondents, and other factors, and we took steps to minimize these errors. We conducted a nonresponse bias analysis to determine whether certain cloud service providers might have been more or less likely to respond to the survey than others. Specifically, we examined whether a cloud service provider's service model (e.g., Software as a Service, Infrastructure as a Service, Platform as a Service),

¹The 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)).

impact level (e.g., high, moderate, low), or deployment model (e.g., government, hybrid, private) was related to whether the CSP responded to the survey. We found that a higher share of cloud service providers that provide Software as a Service (SaaS) responded to the survey than those that provide Infrastructure as a Service (IaaS). In addition, we found that a higher share of cloud service providers that deployed in the government community cloud responded to the survey than those that deployed in the public cloud. These results suggest that cloud service providers that utilize certain service or deployment models were more likely to reply to the survey than others. As a result, the responses of the cloud service provider survey represent only those cloud service providers that participated in this survey, and are not generalizable to cloud service providers as a whole. Despite these limitations, the survey results provide insight into the experiences and views of cloud service providers that did respond.

In addition to the surveys, to address our first objective, we examined 2017, 2018, and 2019 Joint Authorization Board (JAB) and agency authorization data from the 24 agencies to determine if there were an increase, decrease, or no change in the usage of the program. We also interviewed knowledgeable officials from the 24 agencies and FedRAMP PMO to obtain their views on the program.

To address our second objective, we selected four agencies from the 24 agencies based on those with the highest and lowest amount of FedRAMP PMO reported FedRAMP authorizations as of June 15, 2017. We selected the four agencies by dividing them into three equal groups of eight agencies based on the highest to lowest number of FedRAMP PMO reported service authorizations. We selected at least one agency with the highest number of authorizations through FedRAMP in each group, unless we conducted prior FedRAMP work with the agency. Given that two agencies in the third group had the same number of services authorized, we selected both agencies as one had a higher number of reported provisional authorizations through the FedRAMP Joint Authorization Board process and the other had the higher number of reported authorizations through the FedRAMP agency process. To avoid a duplication of our efforts given limited resources, we excluded DOD because another GAO team was reviewing the department's cloud-related efforts, which included leveraging FedRAMP authorizations.

As a result, we selected the Department of Health and Human Services, General Services Administration, the Environmental Protection Agency, and the United States Agency for International Development for our

review. Because HHS is a large federated agency, we selected three operating divisions for a more detailed review. The three operating divisions included the Centers for Disease Control and Prevention (CDC), Centers for Medicare and Medicaid (CMS), and National Institutes of Health (NIH). We selected these divisions based on their extensive usage of cloud service providers authorized through FedRAMP.

To select the agency systems' authorization packages for review, we first identified six cloud services based on FedRAMP PMO data that indicated as of June 15, 2017, the 24 agencies used these cloud services the most. We then requested the selected agencies to provide us with an inventory of systems that relied on the six cloud services in fiscal years 2017 and 2018. From these inventories, we selected 10 agency systems. However, due to sensitivity concerns, we are not disclosing the names of the systems in this report.

The case studies we selected are not generalizable to the other agencies covered by the *Chief Financial Officers Act*. However, it may show the potential FedRAMP issues other agencies face.

For each agency system, we reviewed security authorization documentation, including:

- cloud service provider documentation, such as the Control Implementation Summary on agency and cloud service provider responsibilities to determine the extent agencies documented selected core controls and consistently documented responsibilities in the system security plan;²
- security plans to determine the extent to which plans documented and implemented selected identified core security controls, and met FedRAMP and National Institute of Standards and Technology (NIST) elements;
- security assessment reports to determine if the effectiveness of selected core controls had been assessed and operating as intended;
- the extent to which agencies documented remedial action plans for selected systems to determine if they met FedRAMP or Office of Management and Budget (OMB) elements; and

²Guidance for using FedRAMP states that core controls are controls that support continuous monitoring and must be re-tested at least annually.

- authorization letters to determine the extent appropriate officials approved a cloud service and agency system for use.

To select identified core controls as part of our authorization documentation review, we identified and selected 24 security controls from the 97 identified core controls. Then, to determine the agencies' compliance with the FedRAMP authorization process to assure the protection of agency data, we compared the authorization documentation with the *Federal Information Security Modernization Act of 2014*, the Federal Risk and Authorization Management Program guidance, including the program's Security Assessment Framework, OMB guidance, and NIST Special Publication 800-53 Revision 4.³ Each authorization package area was examined and reviewed by an analyst and each conclusion was corroborated by a second analyst. Where there was disagreement in the assessment, analysts discussed their analysis and reached a consensus.

In addition, we interviewed security representatives and management officials from our selected agencies to determine the effectiveness of the FedRAMP authorization process in reviewing the controls necessary for securing agency data in the cloud, and potential rationale for deficiencies identified in authorization documentation. We also interviewed FedRAMP PMO and OMB staff on their efforts related to the FedRAMP authorization process.

To address our second and third objectives, we also interviewed JAB technical representatives to obtain their views on the benefits and challenges of FedRAMP. Additionally, we obtained information about how the JAB technical representatives reviewed authorization packages.

To determine the reliability of the data used to select agencies and of other data to address our three objectives, we assessed the following:

- FedRAMP program management office points of contact list provided for active cloud service providers and federal agency users of FedRAMP,

³National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, SP-800-53, Revision 4 (Gaithersburg, MD: April 2013).

- FedRAMP program management office data on the 24 CFO Act agencies' fiscal years 2017, 2018, and 2019 JAB and agency authorizations,
- FedRAMP program management office data on cloud service provider participation and agency usage of FedRAMP as of June 15, 2017,
- Agency inventory of systems relying on selected cloud services,
- Cloud service provider authorization documentation contained within secure website portals,
- Cloud service provider and agency reported third-party assessment organizations' security assessment reports, and
- Agency plans of actions and milestones.

To assess the reliability of the information received and reviewed on the FedRAMP marketplace, we collected and reviewed information on agencies' quality control procedures and asked program officials relevant questions on the FedRAMP authorization log standard operating procedure. We reviewed GSA program officials' responses to our data reliability questions such as: how the information was generated, how current the data provided was, how frequently it was updated, and how the data was accurately and consistently entered into the system used. The limitation FedRAMP officials noted was that the data generated was based on voluntarily provided authorization to operate letters submitted to the FedRAMP program management office by each of the CFO Act agencies.

To ensure that the agency systems we reviewed relied on selected cloud service provider products, we had agencies confirm their use of the service supporting the agency's system. We then compared the selected services with agencies' annual FISMA reporting to OMB along with system security documentation (e.g. system security plans) to determine whether the cloud service services we selected were applicable to the selected agency system. A limitation with this method of selection is if an agency's inventory is inaccurate, we would need to reselect a system. For this review, one agency's inventory and system was incomplete resulting in removing that agency system from our selection.

To confirm agencies' virtual access to packages in OMB's repository or a cloud service provider's repository, we obtained screen captures of web portal contents from the FedRAMP PMO. We compared these screen captures with our own virtual access to the packages. We also obtained additional information from the FedRAMP PMO on how it ensures the

accuracy and reliability of the cloud service provider package information. One limitation of this method is that cloud service providers could update documentation where access was outside of OMB MAX portal, and the PMO may not be immediately aware of package updates.

To verify the accuracy and reliability of plans of actions and milestones provided by agencies, we compared the agency's plans of actions and milestones with required OMB elements.⁴ We also requested that agencies describe how they generated the plans of action and milestones provided to us, identify the quality control procedures used, and any limitations to the data they provided.

We evaluated the materiality of the information we obtained and compared it to our audit objectives. We assessed the reliability of the information by reviewing related documents and internal controls such as agency policies and procedures as well as examining packages stored in OMB's MAX portal and cloud service provider repositories. We also interviewed knowledgeable agency officials. Through these methods, we concluded that the information was sufficiently reliable for the purposes of our reporting objectives.

We conducted this performance audit from November 2016 to December 2019 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.

⁴Office of Management and Budget, *Guidance for Preparing and Submitting Security Plans of Actions and Milestones* (Washington, D.C.: Oct. 17, 2001).

Appendix II: FedRAMP Roles and Responsibilities

Table 6: Roles and Responsibilities of FedRAMP Governance Entities

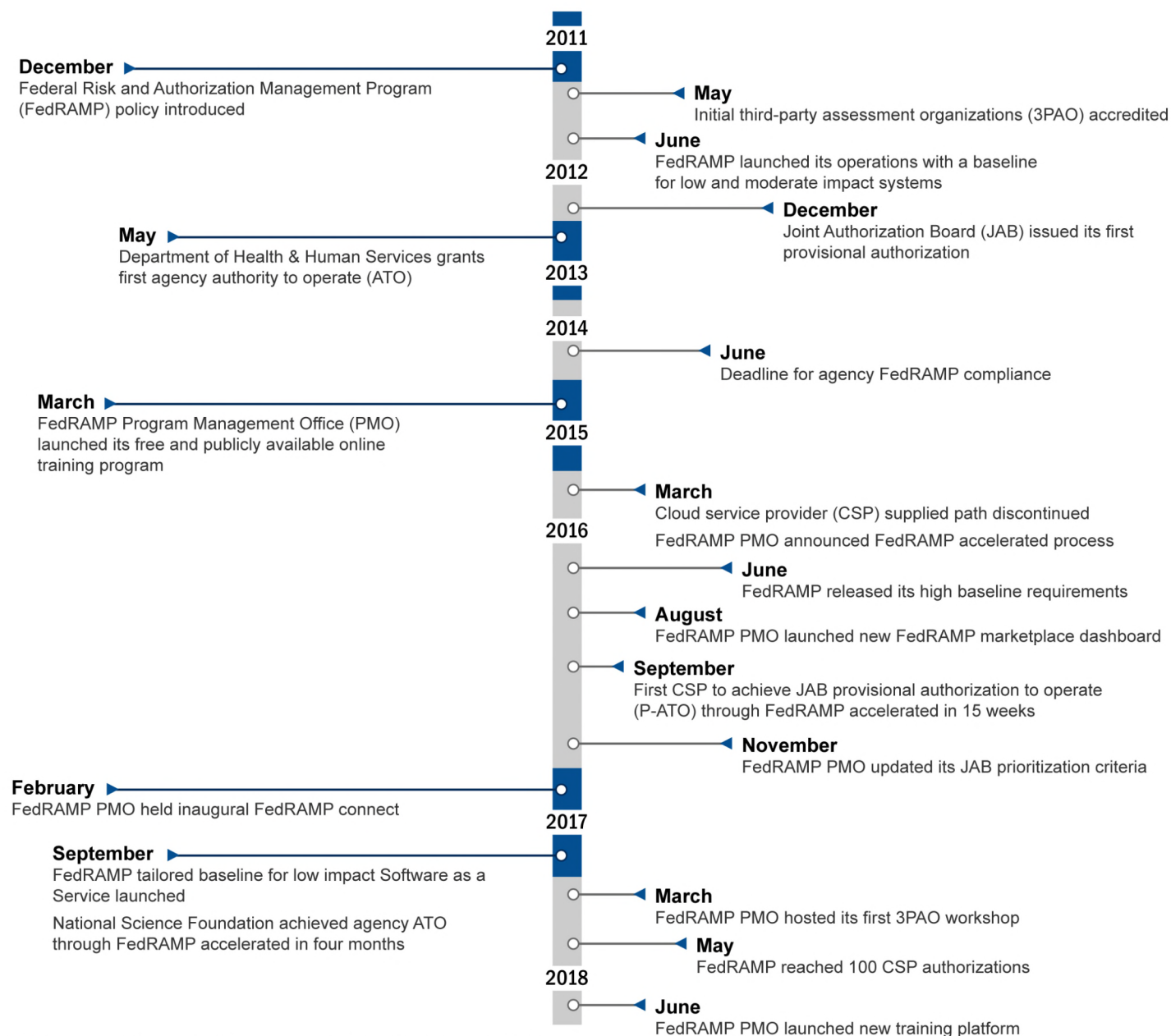
FedRAMP governance entity	Roles and responsibilities
Office of Management and Budget	Issues policies which define the key requirements and capabilities of the FedRAMP program. Oversees and reports on agencies' implementation of information security requirements, including implementation of FedRAMP.
FedRAMP Program Management Office	Develops processes for agencies and providers to request FedRAMP security authorization; Creates a framework for agencies to leverage security authorization packages; Establishes a centralized and secure repository for authorization packages that agencies can leverage to grant security authorizations; Coordinates with the National Institute of Standards and Technology (NIST) and American Association for Laboratory Accreditation to implement a formal conformity assessment to accredit assessors; Develops templates for standard contract language and service level agreements , Memorandum of Understanding and/or Memorandum of Agreement; and Is led by GSA and serves as a liaison to ensure effective communication among all participants.
Joint Authorization Board	Defines and updates the FedRAMP security authorization requirements; Approves accreditation criteria for third-party assessment organizations; Reviews security assessment packages of cloud service providers to grant provisional authorizations; Ensures provisional authorizations are reviewed and updated regularly; and Notifies agencies of changes to or removal of provisional authorizations.
National Institute of Standards and Technology	Advises FedRAMP on FISMA compliance guidance and assists in developing the standards for the accreditation of independent third-party assessment organizations (3PAO).
Federal Chief Information Officers Council	Distributes FedRAMP information to federal CIOs and other representatives through cross-agency communications and events.
Department of Homeland Security	Assists government-wide and agency-specific efforts to provide adequate, risk-based and cost-effective cyber security; Coordinates cyber security operations and incident response; Develops continuous monitoring standards for ongoing cyber security of federal Information systems; and Develops guidance on agency implementation of the Trusted Internet Connection program with cloud services.

Legend: FedRAMP = Federal Risk and Authorization Management Program

Source: GAO review of FedRAMP documentation. | GAO-20-126

Appendix III: FedRAMP Milestones

Figure 6: Federal Risk and Authorization Management Program (FedRAMP) Key Events, December 2011-June 2018



Source: GAO analysis based on FedRAMP Program Management Office's data. | GAO-20-126

Appendix IV: Comments from the General Services Administration



The Administrator

October 17, 2019

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

Dear Mr. Dodaro:

The U.S. General Services Administration (GSA) appreciates the opportunity to review *Cloud Computing Security: Agencies Increased Use of Federal Authorization Program, but Improved Oversight and Implementation Needed* (GAO19-383), which includes a review of GSA's Federal Risk and Authorization Management Program (FedRAMP). FedRAMP provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

FedRAMP aims to empower agencies to modernize operations using secure cloud solutions to improve agencies' information technology security. GSA is committed to continuous improvement of the authorization and continuous monitoring processes, as well as to guidance and outreach with stakeholders.

GSA reviewed this report, agrees with the recommendations (Appendix A), and is developing a plan to address the recommendations made to GSA. The agency is confident that these actions will satisfactorily remedy the concerns raised by GAO.

If you have any questions, please contact me at (202) 969-7277 or Jeffrey A. Post, Associate Administrator, Office of Congressional and Intergovernmental Affairs, at (202) 501-0563.

Sincerely,

A handwritten signature in blue ink that reads "Emily W. Murphy".

Emily W. Murphy
Administrator

cc: Gary C. Wilshusen, Director, Information Security Issues, GAO

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

2

Appendix A

Recommendation 2: The Administrator of the General Services Administration should direct the Acting Director of FedRAMP to clarify guidance to agencies and cloud service providers on program requirements and responsibilities

Recommendation 3: The Administrator of the General Services Administration should direct the Acting Director of FedRAMP to improve the program's continuous monitoring process by allowing more automated capabilities, including for agencies to review documentation.

Recommendation 4: The Administrator of the General Services Administration should update security plans for selected systems to include the description of security controls and plan reviews and approvals.

Recommendation 5: The Administrator of the General Services Administration should update the security assessment report for the selected system to identify the summarized results of control effectiveness tests.

Recommendation 6: The Administrator of the General Services Administration should update the list of corrective actions for selected systems to identify the responsible office and estimated funding required and anticipated source of funding.

Recommendation 7: The Administrator of the General Services Administration should develop guidance requiring that cloud service authorization letters be provided to the FedRAMP program management office.

Appendix V: Comments from the Department of Health and Human Services



DEPARTMENT OF HEALTH & HUMAN SERVICES

Office of the Secretary

Assistant Secretary for Legislation
Washington, D.C. 20201

Gregory Wilshusen
Director of Information Security Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

OCT 18 2019

Dear Mr. Wilshusen,

Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled, *"Cloud Computing Security: Agencies Increased Use of Federal Authorization Program, but Improved Oversight and Implementation Needed"* (GAO-19-383).

The Department appreciates the opportunity to review this report prior to publication. We will work with our Operating Divisions towards addressing Recommendations 8-18. HHS looks forward to continuing to mature our cloud security and FedRAMP program and facilitate increased FedRAMP awareness throughout the agency.

Sincerely,

A handwritten signature in black ink, appearing to read "S. Arbes", is written over a horizontal line.

Sarah Arbes
Assistant Secretary for Legislation

Attachment

GENERAL COMMENTS FROM THE DEPARTMENT OF HEALTH & HUMAN SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED – CLOUD COMPUTING SECURITY: AGENCIES INCREASED USE OF FEDERAL AUTHORIZATION PROGRAM, BUT IMPROVED OVERSIGHT AND IMPLEMENTATION NEEDED (GAO-19-383)

Recommendation 8

The Secretary of Health and Human Services should:

- Direct the Director of the Centers for Disease Control and Prevention (CDC) to update the security plan for the selected system to identify the authorization boundary, the system operational environment and connections, a description of security controls, and the individual reviewing and approving the plan and date of approval.

HHS Response

CDC generally concurs with GAO's recommendation. CDC is currently revising its cybersecurity policies and procedures that will specifically address the FedRAMP security control assessment and documentation deficiencies described. CDC will use updates to the selected system's security authorization package as a pilot for greater programmatic improvements.

Additionally, CDC notes that GAO's observations were narrowly focused on specific authorization artifacts and did not fully take into account CDC's established, FISMA compliant authorization processes and procedures. For example, GAO's observation that the SSP was not "Reviewed and approved by authorizing official" is based on the fact that the system security plan (SSP) was not signed by the authorizing official (AO). However, CDC prepares and presents authorization artifacts to the authorizing official as a complete authorization package. This package includes the final SSP as well as the security assessment report (SAR) and the authorization letter (to be signed by the AO). Thus, the AO signature on the authorization letter covers all required documents in the authorization package including the SSP. Similarly, the authorization boundary information that GAO did not find in the SSP was included in the SAR, which is signed by the certification agent.

Recommendation 9

The Secretary of Health and Human Services should:

- Direct the Director of the CDC to update the security assessment report for the selected system to identify the summarized results of control effectiveness tests.

HHS Response

CDC generally concurs with GAO's recommendation. CDC is currently revising its cybersecurity policies and procedures that will specifically address the FedRAMP security control assessment and documentation deficiencies described in this recommendation and will use updates to the selected system's security authorization package as a pilot for greater programmatic improvements.

CDC also notes that GAO's observations were narrowly focused on specific authorization artifacts and did not fully take into account CDC's established, FISMA compliant authorization processes and procedures. For example, GAO found that CDC's SAR only reported control weaknesses and did not address controls that were operating effectively. However, CDC's security control assessments adhere to NIST SP 800-53A requirements, document the details of all security assessments in CDC's Governance, Risk, and Compliance tool, Trusted Agent, and summarize the test results of every control (passed and failed) in the final SSP. CDC's SAR is designed to highlight the details of failed or unimplemented controls in order to ensure the CA and AO are aware of these verified control weaknesses when making risk-based authorization decisions.

GENERAL COMMENTS FROM THE DEPARTMENT OF HEALTH & HUMAN SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED – CLOUD COMPUTING SECURITY: AGENCIES INCREASED USE OF FEDERAL AUTHORIZATION PROGRAM, BUT IMPROVED OVERSIGHT AND IMPLEMENTATION NEEDED (GAO-19-383)

Recommendation 10

The Secretary of Health and Human Services:

- Direct the Director of the CDC to update the list of corrective actions for the selected system to identify the specific weaknesses, funding source, changes to milestones and completion dates, identified source of weaknesses, and status of corrective actions.

HHS Response

CDC generally concurs with GAO's recommendation. CDC is currently revising its cybersecurity policies and procedures that will specifically address the FedRAMP security control assessment and documentation deficiencies described in this recommendation and will use updates to the selected system's security authorization package as a pilot for greater programmatic improvements.

Additionally, CDC would like to note that GAO's observations were narrowly focused on specific authorization artifacts and did not fully take into account CDC's established, FISMA compliant authorization processes and procedures. For example, GAO found that CDC's Plans of Action and Milestones (POA&M) did not include key elements. However, CDC's weakness management process is compliant with both Federal requirements and HHS POA&M management standards. Details regarding the status of POA&M milestones are captured and tracked in CDC's Governance, Risk, and Compliance tool, Trusted Agent and are shared with HHS on a monthly basis.

Recommendation 11

The Secretary of Health and Human Services should action:

- Direct the Administrator of the Centers for Medicare and Medicaid Services (CMS) to update the security plan for the selected system to identify the authorization boundary, the system operational environment and connections, a description of security controls, and the individual reviewing and approving the plan and date of approval.

HHS Response

CMS concurs with GAO's recommendation. CMS will update the system security plans for the selected systems to address this finding.

Recommendation 12

The Secretary of Health and Human Services should:

- Direct the Administrator of CMS to update the security assessment report for the selected system to identify the summarized results of control effectiveness tests.

GENERAL COMMENTS FROM THE DEPARTMENT OF HEALTH & HUMAN SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED – CLOUD COMPUTING SECURITY: AGENCIES INCREASED USE OF FEDERAL AUTHORIZATION PROGRAM, BUT IMPROVED OVERSIGHT AND IMPLEMENTATION NEEDED (GAO-19-383)

HHS Response

CMS concurs with GAO's recommendation. During 2017, the assessment that was performed by CMS was an internal assessment. This limited scope assessment is one portion of an overall Information Security Program to help management determine the security risks this application presents to CMS. As a result, the assessment report was not in a standard format. Going forward, CMS will follow the requirements set forth by the CMS Acceptable Risk Safeguards (ARS) security control, CA-02 Security Assessments, which requires that a security assessment report documents the results of the assessment (pass/fail for each control tested).

Recommendation 13

The Secretary of Health and Human Services should:

- Direct the Administrator of CMS to update and document the CMS remedial action plans for the selected systems to identify the specific weakness, responsible office, estimated funding required, and changes to milestone completion dates.

HHS Response

CMS concurs with GAO's recommendation. As part of CMS remedial action plans for tracking the resolution of system issues, CMS follows OMB requirements for specific information that should be included. CMS will review the remedial action plans for the selected system and update to include the funding required.

Recommendation 14

The Secretary of Health and Human Services should:

- Direct the Administrator of CMS to prepare letters authorizing the use of cloud services for the selected systems and submit the letters to the FedRAMP program management office.

HHS Response

CMS concurs with GAO's recommendation. CMS has educated staff to ensure all key components of the FedRAMP authority to operate (ATO) letter, including information on the use of cloud services, is included when preparing authorization letters and sending to the FedRAMP program management office.

Recommendation 15

The Secretary of Health and Human Services should:

- Direct the Director of the National Institutes of Health (NIH) to update the security plan for the selected system to identify the authorization boundary, system operation in terms of mission and business processes, operational environment and connections, and a description of security controls.

HHS Response

The NIH concurs with GAO's recommendation. The NIH will provide an action plan to address the recommendation in our 180-day letter response to Congress.

GENERAL COMMENTS FROM THE DEPARTMENT OF HEALTH & HUMAN SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED – CLOUD COMPUTING SECURITY: AGENCIES INCREASED USE OF FEDERAL AUTHORIZATION PROGRAM, BUT IMPROVED OVERSIGHT AND IMPLEMENTATION NEEDED (GAO-19-383)

Recommendation 16

The Secretary of Health and Human Services should:

- Direct the Director of the NIH to update the security assessment report for the selected system to identify the summarized results of control effectiveness tests.

HHS Response

The NIH concurs with GAO's recommendation. The NIH will provide an action plan to address the recommendation in our 180-day letter response to Congress.

Recommendation 17

The Secretary of Health and Human Services should:

- Direct the Director of the NIH to update the list of corrective actions for the selected system to identify estimated funding and anticipated source of funding, key milestones with completion dates, and changes to milestones and completion dates.

HHS Response

The NIH concurs with GAO's recommendation. The NIH will provide an action plan to address the recommendation in our 180-day letter response to Congress.

Recommendation 18

The Secretary of Health and Human Services should:

- Direct the Director of NIH to submit the division's letters authorizing the use of cloud services for the selected systems to the FedRAMP program management office.

HHS Response

The NIH concurs with GAO's recommendation. The NIH will provide an action plan to address the recommendation in our 180-day letter response to Congress.

Appendix VI: Comments from the Environmental Protection Agency



UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

NOV 6 2019

OFFICE OF MISSION SUPPORT

Mr. Gregory C. Wilshusen,
Director, Information Security Issues
U.S. Government Accountability Office
441 G St., NW
Washington, DC 20548

Dear Mr. Wilshusen:

Thank you for the opportunity to review and comment on the GAO Draft Report, 19-383, *Cloud Computing Security: Agencies Increased Use of Federal Authorization Program, but Improved Oversight and Implementation Needed* (101221).

The purpose of this letter is to provide the Environmental Protection Agency's (EPA's) response to the findings and recommendations in GAO's Draft Report.

In the Draft Report, GAO recommended:

Recommendation 19:

The Administrator of the Environmental Protection Agency should update security plans for selected systems to identify a description of security controls, and the individual reviewing and approving the plan and date approval.

EPA Response: The EPA disagrees with this finding. One system selected for review was not in production and was not used for EPA operations. For systems used for operations, the EPA Chief Information Security Officer will coordinate with agency Information Security Officers to ensure system security plans include all required information. The CISO will monitor all systems for compliance through the established Chief Information Officer Authorization to Operate process.

Recommendation 20:

The Administrator of the Environmental Protection Agency should update the security assessment report for the selected system to identify the summarized results of control effectiveness tests.

EPA Response: The EPA disagrees with this finding. One system selected for review was not in production and was not used for EPA operations. For the other system reviewed, the EPA used a FedRAMP certified Third Party Assessor that provided full documentation of control test results.

Recommendation 21:

The Administrator of the Environmental Protection Agency should update the list of corrective actions for selected systems to identify the specific weakness, estimate funding and anticipated source of funding, key remediation milestones with completion dates, changes to milestones and completion dates, and source of the weakness.

EPA Response: The EPA partially agrees with this finding. One system selected for review was not in production and was not used for EPA operations. For systems used for operations, the EPA Chief Information Security Officer will coordinate with agency Information Security Officers to ensure corrective actions have plans of actions and milestones as appropriate that include all required information. The CISO will monitor all systems for compliance through the established Chief Information Officer Authorization to Operate process.

Recommendation 22:

The Administrator of the Environmental Protection Agency should prepare letters authorizing the use of cloud services through the selected systems and submit the letters to the FedRAMP program management office.

EPA Response: The EPA disagrees with this recommendation. One system selected for review was not in production and was not used for EPA operations. For the other system, an authorization letter could not be retrieved for a timeframe, however, the system does have a current authorization to operate and the Agency does prepare and use authorization documents for cloud services. The Agency does submit authorization documents to the FedRAMP program management office (PMO). The footnote in the GAO's reports states that the authorization document sent to the FedRAMP PMO did not clearly identify the specific service authorized. Even though the footnote also states that the Agency did send the authorization letters to the FedRAMP PMO, the GAO indicates the EPA did not forward the authorization document to the FedRAMP PMO, when in fact it was forwarded in accordance with published FedRAMP PMO guidance. The FedRAMP PMO guidance, to include their authorization letter example, does not stipulate including the specific service authorized. The EPA will continue to follow, as appropriate, FedRAMP PMO guidance promulgated through the General Services Administration FedRAMP Website.

Recommendation 23:

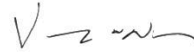
The Administrator of the Environmental Protection Agency should develop guidance requiring that cloud services authorization letters be provided to the FedRAMP program management office.

**Appendix VI: Comments from the
Environmental Protection Agency**

EPA Response: The EPA disagrees with this recommendation. The EPA has a standard operating procedure where the EPA Chief Information Security Officer forwards authorization letters to the FedRAMP Program Management Office.

If you require additional information or would like to discuss further, please contact Patricia Randolph Williams at (202) 564-0204.

Sincerely,



Vaughn Noga
Chief Information Officer and
Deputy Assistant Administrator for Environmental
Information

cc: Patricia Randolph Williams, OMS
Janice Jablonski, OMS
Robert McKinney, OISP
Bill Sabbagh, OMS IO
Jeff Anouilh, OISP
Lee Kelly, OISP
Torina Anderson, OISP
Marcus Green, OISP
Annette Morant, OCFO
Larry Crosland, GAO

Appendix VII: Comments from the U.S. Agency for International Development



October 15, 2019

Gregory C. Wilshusen
Director, Information-Security Issues
U.S. Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20226

Re: CLOUD COMPUTING SECURITY: Agencies Increased Use of Federal Authorization Program, but Improved Oversight and Implementation Needed. (GAO-19-383)

Dear Mr. Wilheusen:

I am pleased to provide the formal response of the U.S. Agency for International Development (USAID) to the draft report produced by the U.S. Government Accountability Office (GAO) titled, *CLOUD COMPUTING SECURITY: Agencies Increased Use of Federal Authorization Program, but Improved Oversight and Implementation Needed* (GAO-19-383).

USAID is committed to improving the security of our information systems that support our mission and business functions, particularly cloud computing. The Agency is a leader in modernizing information technology (IT) among Federal Departments and Agencies, having adopted cloud-based platforms for email and services, implemented IT collaboration tools, and migrated to a new cloud data center and disaster-recovery site. We are also improving our cloud-computing program in response to the recommendations of the GAO's draft report, as follows:

USAID has already addressed all or part of two of the recommendations in the draft report, as stated in our response to the GAO's Statement of Facts for this audit, submitted on July 11, 2019. First, USAID has updated Plans of Action and Milestones (POA&Ms) that address the parties responsible for weaknesses for the system selected for review in the audit ("System 10"), as submitted in our response to the GAO's Statement of Facts for the draft report on July 11, 2019. USAID is also updating our policy for managing POA&Ms to address the remainder of the draft report's recommendation in this area, and we are tracking the source of weaknesses in POA&Ms.

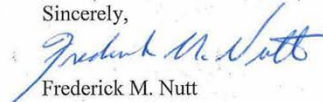
Second, USAID acknowledges the improvements we needed to make to prepare the Authorization to Operate (ATO) Letter to authorize the use of cloud services for System 10 and submit it to the program-management office for the Federal Risk Authorization Management Program (FedRAMP). To that end, USAID has already submitted the ATO Letter for "System 10" to FedRAMP, and has established a process in the *USAID Information Technology (IT) Systems Accreditation Risk-Management Framework (RMF) Handbook* to prepare such ATO Letters that authorize the use of cloud services for systems. On September 19, 2019, we issued an Agency Notice to announce the document's publication.

**Appendix VII: Comments from the U.S. Agency
for International Development**

Nevertheless, our lack of visibility into the FedRAMP system in question and restrictions under FedRAMP's Non-Disclosure Agreements or Terms of Access and Use constrain our ability to provide a more complete response to one of the draft report's recommendations. A full explanation appears in the enclosure.

I am transmitting this letter and the enclosed comments from USAID for inclusion in the GAO's final report. Thank you for the opportunity to respond to the draft report, and for the courtesies extended by your staff while conducting this engagement. We appreciate the opportunity to participate in the complete and thorough evaluation of our interactions with FedRAMP for authorizing cloud services.

Sincerely,



Frederick M. Nutt
Assistant Administrator
Bureau for Management

Enclosure: a/s

**COMMENTS BY THE U.S. AGENCY FOR INTERNATIONAL DEVELOPMENT ON
THE DRAFT REPORT PRODUCED BY THE U.S. GOVERNMENT
ACCOUNTABILITY OFFICE (GAO) TITLED, CLOUD COMPUTING SECURITY:
Agencies Increased Use of Federal Authorization Program, but Improved Oversight and
Implementation Needed. (GAO-19-383)**

The U.S. Agency for International Development (USAID) would like to thank the U.S. Government Accountability Office (GAO) for the opportunity to respond to this draft report. We appreciate the extensive work of the GAO engagement team, and the specific findings that will help USAID achieve greater effectiveness in the oversight and implementation of security requirements for cloud computing.

The draft report contains three recommendations for USAID (Recommendations 24, 25, and 26). We concur with Recommendations 25 and 26, but do not concur with Recommendation 24. Additionally, USAID partially addressed Recommendation 25 in our response to the GAO's Statement of Facts for this audit, which we submitted on July 11, 2019.

The following are USAID's detailed responses to the draft report's recommendations:

- 1. The Administrator of USAID should update the system security plan for the selected system to identify the authorization boundary, the system operational environment and connections, and a description of security controls. (Recommendation 24)*

USAID disagrees with Recommendation 24, as stated in our response to the GAO's Statement of Facts, and the Agency will request that the GAO close this recommendation upon the issuance of the Final Report. USAID's response on Recommendation 24, as articulated at the Exit Conference for the draft report, appears below:

The GAO's Recommendation: Describe the authorization boundary for the selected system ("System 10").

USAID's response: USAID described the authorization boundary for System 10 with the Federal Risk Authorization Management Program (FedRAMP) Cache Tool on page 10 of the System Security Plan (SSP) for System 10. In the SSP diagram for System 10 the Agency provided to the GAO during the fieldwork stage of this audit, a gray line separates the FedRAMP Cache Tool from the system's boundary, which indicates that the FedRAMP Cache Tool is outside of the boundary. USAID uses the FedRAMP Cache Tool as a customer. According to the non-disclosure agreement (NDA) with FedRAMP, customers can view FedRAMP information on MAX.gov, but do not have the right to share or copy this information. The information USAID includes in the SSP for System 10 is limited to USAID, and the FedRAMP-specific information for the system remains with the FedRAMP program, according to the NDA and FedRAMP's Terms of Access and Use. Therefore, in compliance with FedRAMP's Terms

of Access and Use, USAID could only include information about the FedRAMP Cache Tool at a high level in the SSP (on pages 10 and 13 of the document). There is no further information not already included in the current SSP for System 10 we can add to describe the authorization boundary, as we are not permitted to include FedRAMP details in the Agency's SSP. USAID respectfully requests for the GAO to remove this recommendation in the Final Report or close it upon issuance.

The GAO's Recommendation: Document the operational environment and connections for System 10.

USAID's response: USAID does document the FedRAMP operational environment and connections for System 10 to the extent required. As a customer of FedRAMP, USAID only addresses the *customer-side* operational environment and connections for System 10. FedRAMP provides its own documentation on *its* operational environment and connections. There is no further information not already included in the current SSP for System 10 we can add to describe its operational environment and connections, as we are not permitted to include FedRAMP details in the Agency's SSP.

The GAO's Recommendation: Describe the implementation of security controls for System 10, including the Agency's responsibility identified in the control-implementation summary. In the Exit Conference held on July 11, 2019, the GAO explained this finding further by stating that the IR-2 control in the SSP is not addressed fully because the statement reads, "This control is inherited from the Information Assurance (IA) Common Controls."

USAID's response: In the SSP for System 10, USAID has already documented the security controls for which the Agency is responsible. Additionally, we have developed an Agency-wide Common-Controls Matrix that lists common controls a system can inherit from the Agency. The Agency has addressed these common controls in the IA Common-Controls SSP, and provided the document to the GAO on July 11, 2019, in our response to the GAO's Statement of Facts for this audit. There is no further information not already included in the current SSP for System 10 we can add to describe the implementation of security controls for System 10, as we are not permitted to include FedRAMP details in the Agency's SSP.

2. *The Administrator of USAID should update the list of corrective actions for the selected system to include the party responsible for addressing the weakness, and source of the weakness. (Recommendation 25)*

USAID has addressed Recommendation 25 partially. At the Exit Conference for this audit, the Agency submitted approved POA&Ms that identify the parties responsible for weaknesses in System 10. USAID is updating our policy for managing POA&Ms to address the remainder of the recommendation, and we are tracking the source of the weaknesses in POA&Ms. USAID provided the below response to Recommendation 25 in the Exit Conference.

The GAO's Recommendation: Identify the party responsible for addressing weaknesses in System 10.

USAID's Response: USAID did identify the party responsible for addressing weaknesses in System 10, and assigned POA&Ms to the System Owner (SO). The Cybersecurity and Asset-Management (CSAM) tool does not allow for the approval of POA&Ms if the section on Assigned Parties is not filled out. The GAO might have reviewed the draft POA&Ms before they were final, which would explain why information was missing. USAID provided the GAO with final, approved POA&Ms for System 10 on July 11, 2019.

3. *The Administrator of USAID should prepare the letter authorizing the use of cloud service for the selected system and submit the letter to the FedRAMP program management office. (Recommendation 26)*

USAID acknowledges the improvements we must make to meet Recommendation 26. To that end, the Agency has already established a process in the *USAID Information Technology (IT) Systems Accreditation Risk-Management Framework (RMF) Handbook* to prepare letters that authorize the use of cloud services for systems. USAID issued an Agency Notice to announce the publication of the document on September 19, 2019. In addition, USAID has already submitted the Authorization to Operate Letter for System 10 to FedRAMP, and therefore will be requesting that the GAO close this recommendation upon the issuance of the Final Report.

Appendix VIII: Comments from the Department of Veterans Affairs



DEPARTMENT OF VETERANS AFFAIRS
WASHINGTON DC 20420

OCT 04 2019

Mr. Gregory C. Wilshusen
Director
Information Security Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Wilshusen:

The Department of Veterans Affairs (VA) has reviewed the Government Accountability Office's (GAO) draft report, ***Cloud Computing Security: Agencies Increased Use of Federal Authorization Program, but Improved Oversight and Implementation Needed*** (GAO-19-383). While GAO has no findings or recommendations addressed to the Department, VA generally concurs with the information and findings presented in the draft report.

VA remains committed to maintaining the security of the VA Enterprise Cloud environment in compliance with the requirements of the Federal Information Security Modernization Act of 2014. Further, VA recognizes the benefits of the Federal Risk and Authorization Management Program (FedRAMP) for selecting and authorizing the use of cloud services that meet Federal security requirements. VA policy also requires compliance with FedRAMP for all cloud deployments.

VA appreciates the opportunity to review the draft report.

Sincerely,

A handwritten signature in blue ink, appearing to read "Pamela Powers".

Pamela Powers
Chief of Staff

Appendix IX: Comments from the Social Security Administration



SOCIAL SECURITY
Office of the Commissioner

October 15, 2019

Gregory C. Wilshusen
Director, Information Security Issues
United States Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Director Wilshusen:

Thank you for the opportunity to review the draft report, "CLOUD COMPUTING SECURITY: Agencies Increased Use of Federal Authorization Program, but Improved Oversight and Implementation Needed" (GAO-19-383). We have no comment.

If you have any questions, please contact me at (410) 965-9704. Your staff may contact Trae Sommer, Director of the Audit Liaison Staff, at (410) 965-9102.

Sincerely,

Stephanie Hall
Deputy Chief of Staff

SOCIAL SECURITY ADMINISTRATION BALTIMORE, MD 21235-0001

Appendix X: GAO Contact and Staff Acknowledgments

GAO Contact

Gregory C. Wilshusen, (202) 512-6244 or wilshuseng@gao.gov.

Staff Acknowledgments

In addition to the individual named above, Sara Ann W. Moessbauer, (Director), Larry Crosland (Assistant Director), Rosanna Guerrero (Analyst-in-Charge), Sher'rie Bacon, Nabajyoti Barkakati, Christina Bixby, David Blanding, Chris Businsky, Fatima Jahan, David Plocher, Dana Pon, Carl Ramirez, Cynthia Saunders, and Priscilla Smith made significant contributions to this report.

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 GAO's website (<https://www.gao.gov>). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to <https://www.gao.gov> and select "E-mail Updates."

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 [E-mail 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/fraudnet/fraudnet.htm>

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

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@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

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



Please Print on Recycled Paper.