

GAO Highlights

Highlights of [GAO-20-126](#), a report to congressional requesters

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.

December 2019

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.