ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

Reforming FedRAMP: A Guide to Improving the Federal Procurement and Risk Management of Cloud Services

MICHAEL MCLAUGHLIN I JUNE 2020

FedRAMP—the government program that sets standards for assessing, authorizing, and monitoring the security of cloud systems—can significantly improve. Absent reform, it will hamper agencies' adoption of cloud services.

KEY TAKEAWAYS

- Despite improvements to FedRAMP, procuring cloud computing services at the federal level is still too slow, too costly, and inconsistent across agencies.
- These issues have created barriers for businesses offering cloud services to the government and have slowed agencies' access to technology that increases their operational efficiency and reduces costs.
- Policymakers have recommended reforms, but Congress and the administration should do more to improve FedRAMP and provide it with the necessary funding to hire more people to review cloud services promptly.
- FedRAMP should require agencies to re-use existing authorizations for a cloud service, establish leads at each federal agency, and implement pilot programs to experiment with ways to overhaul how FedRAMP reviews and authorizes cloud services.

INTRODUCTION

Since its creation in 2011, FedRAMP—a program created to provide the federal government a standard approach to evaluating, authorizing, and monitoring the security of cloud systems—has helped many federal agencies procure secure cloud computing services.[1] In turn, the adoption of cloud computing has helped agencies better meet their missions. Nevertheless, despite successful attempts at improving the process, FedRAMP still suffers from long timelines, high costs, and review processes that are inconsistent across federal agencies. These issues have created artificial barriers to businesses offering their services to the federal government, thereby slowing agencies' access to cloud services that increase their ability to serve the public while cutting costs. As such, several individuals have recommended a range of solutions to improve FedRAMP.[2] In particular, Rep. Gerry Connolly (D-VA) and Rep. Mark Meadows (R-NC) have introduced the "Federal Risk and Authorization Management Program Authorization Act of 2019" (FedRAMP Authorization Act), which passed the U.S. House of representatives in February 2020, to reform the program.[3] The bill would make several positive improvements to FedRAMP, but Congress and the administration can and should do even more to fix FedRAMP's flaws.

This report first describes FedRAMP and why lawmakers should care about the effectiveness of the program. It then details the program's positive evolution since 2011, and also its remaining challenges. Next the report analyzes the FedRAMP Authorization Act, and offers recommendations to improve the bill while also suggesting actions that the administration should take now to improve the program.[4]

WHAT IS FEDRAMP?

FedRAMP is the Federal Risk and Authorization Management Program, a program developed jointly by the National Institute of Standards and Technology (NIST), the General Services Administration (GSA), the Department of Defense (DOD), and the Department of Homeland Security (DHS) to provide agencies a standardized approach to assessing, authorizing, and continuously monitoring the security of cloud services.[5] The groups designed FedRAMP to assist agencies in complying with the Federal Information Security Management Act (FISMA) of 2002, which Congress updated in 2014, when using cloud services. FISMA requires agencies to meet appropriate levels of security requirements for their information systems based on the information these systems hold and their organizational needs.[6] At the time of FedRAMP's inception, agencies cited security concerns as a reason to not adopt cloud computing.[7] The program is mandatory for all federal agency cloud deployments, except for those implemented in federal facilities intended for only a single organization.[8] The Joint Authorization Board (JAB), which is made up of the chief information officers (CIOs) of DOD, DHS, and GSA, sets the minimum security requirements for FedRAMP-compliant cloud systems. FedRAMP's requirements are based on security controls NIST has established, and the FedRAMP program management office (PMO) works with the JAB to incorporate the requirements into a security-assessment framework.[9] Besides ensuring security, FedRAMP has goals of enabling federal agencies to rapidly adopt cloud computing in a cost-effective manner.[10]

How Does FedRAMP Work?

Under FedRAMP, there are multiple ways to authorize a cloud service for use at a federal agency. Under any path, however, agencies and cloud services providers (CSPs) must go through several processes. For example, federal agencies must categorize the impact level of the type of system they intend to procure as low, moderate, or high based on the type of information the system will store, process, or transmit.[11] In addition, a third-party assessment organization (3PAO) or independent assessor will test a vendor's cloud system to determine whether it meets the security standards associated with its intended impact level.[12] This assessment includes penetration testing, vulnerability scanning, and the assessment of security controls, which are safeguards that protect the confidentiality, integrity, and availability of information, such as encryption.[13] Vendors may implement new security controls or reconfigure existing controls to meet these requirements.[14]

The most common way to authorize a cloud system under FedRAMP, accounting for roughly 70 percent of initial authorizations, is for an individual agency to issue an authority to operate (ATO).[15] In this path, a CSP works directly with an agency to obtain an authorization. The path involves several phases, including the initial establishment of a partnership, quality and risk review of a CSP's security authorization package—such as the security assessment report from a 3PAO—and the remediation of any security gaps the agency identifies during its review.[16] FedRAMP's agency authorization playbook outlines that this authorization path should take 16–18 weeks.[17] After a cloud provider receives an ATO, it must implement a continuous monitoring capability to ensure the service maintains an acceptable risk posture.[18]

The other authorization path is for a CSP to obtain a JAB provisional authority to operate (P-ATO). In this path, the JAB, rather than a federal agency, conducts an in-depth review of a cloud offering's security authorization package to potentially issue a P-ATO.[19] While a P-ATO offers assurance to agencies that the DOD, DHS, and GSA have reviewed and approved a cloud system, FISMA requires agencies to make their own risk-based determination to provide a security authorization for any IT system.[20] As such, agencies must review the P-ATO package and issue their own ATO.[21] The JAB typically reviews the cloud offerings of three cloud providers a quarter due to resource constraints.[22] The JAB prioritizes reviewing systems it believes could be authorized government wide and has a goal of completing all authorizations within six months.[23]

Agencies can also elect to authorize a cloud service that has already achieved a FedRAMP ATO from another agency. In this scenario, agencies review a cloud service's authorization package, which includes information such as a security assessment report and control implementation summary, to determine whether the service meets the agency's needs. The reuse of packages helps cloud providers and agencies save money, while leading to quicker implementations of technology.[24] For example, if an agency plans to purchase the same services another agency has previously authorized, the agency may not need to undergo several pre-authorization and authorization phases with the CSP, such as remediation of identified risks, that can combine to take more than three months.[25] When using an already FedRAMP-authorized cloud service, an agency knows that a CSP's offering meets FedRAMP requirements.[26] An agency can leverage an existing authorization by using some or all of the information in its package.[27]

The last key element of FedRAMP is the PMO, which resides in GSA and supports the day-to-day operation of the program.[28] The office provides this support in several ways, including creating

templates and offering guidance to agencies and cloud providers. In addition, the PMO manages the accreditation program for 3PAOs and acts as a communications liaison to all stakeholders.[29] Importantly, the PMO also reviews documentation that demonstrates a CSP is ready to go through the JAB P-ATO process, and validates all agency ATOs.[30]

WHY IS FEDRAMP IMPORTANT?

FedRAMP is important because it affects the security of cloud services federal agencies use and the speed in which agencies can procure them. Specifically, FedRAMP ensures agencies acquire cloud services in accordance with FISMA.[31] Recent security breaches in both the public and private sectors—such as the 2015 data breach of the U.S. Office of Personnel Management, in which hackers targeted the personal information of individuals, including Social Security numbers—highlight the importance of information security.[32] FedRAMP's relevance has also increased as state and local governments frequently procure FedRAMP-authorized products and services in part because of their authorization, which implies the products or services are secure.[33]

As of April 2020, there are roughly 150 FedRAMP authorized Software-as-a-Service (SaaS) approved solutions, compared with roughly 12,000 in the private market.

An efficient FedRAMP process makes it easier for agencies to procure secure cloud services, which is important because cloud computing can provide the government significant benefits, including improvements in scalability, efficiency, and security. Scalability is especially important in times of peak demand, such as during a natural disaster or other national emergency, and non-cloud-based applications can be overwhelmed.[34] In contrast, if FedRAMP unnecessarily elongates the procurement process, it slows the adoption of cloud services by agencies. In addition, if FedRAMP's compliance costs are too high, FedRAMP acts as a barrier to entry to firms offering their cloud services to the government. As a result, an inefficient FedRAMP leads to agencies having fewer offerings to choose from compared with their private-sector counterparts, which can hinder them from procuring the best service for their needs.[35] Shortening the time it takes for a product or service to become FedRAMP compliant could both open the federal market to thousands of software providers and enhance agencies' access to innovative technology.[36] It is challenging to specify FedRAMP's exact effect on the availability of cloud services to government agencies, but it is clear there are more services available to private-sector organizations than federal agencies. For example, as of April 2020, there are roughly 150 FedRAMP authorized Software-as-a-Service (SaaS) approved solutions, compared with roughly 12,000 in the private market.[37]

Cloud Computing Is Providing the Government Significant Benefits

Cloud computing provides on-demand access to computing resources, ranging from applications to servers.[38] The most common forms of cloud computing include SaaS, platform as a service (PaaS), and infrastructure as a service (IaaS).[39] SaaS is widely used by Internet users in the United States. For example, web-based email and document editing and sharing applications are both examples of SaaS as users access these applications online through a web browser on a computer or mobile device, rather than through software installed and run on a local desktop or server.[40] PaaS allows users to rent virtualized software development or production environments

("platforms") to run their applications or services. Organizations use PaaS to rapidly and efficiently develop and deploy new applications without having to invest in expensive hardware or software, or manage complex networking and computing infrastructure.[41] As of May 29, 2020, there were 37 FedRAMP-authorized PaaS products and services.[42] IaaS gives organizations of any size access to secure, enterprise-class computing infrastructure that can be efficiently managed and scaled to meet different needs. IaaS allows companies to purchase computing resources on a metered basis, much like they would purchase electricity, water, or any other utility. An example of IaaS is cloud storage, which provides users access to scalable online storage. Other IaaS approaches offer pay-as-you-go pricing for computing, data transfers, and content distribution networks.[43] As of May 27, 2020, there were 25 FedRAMP-authorized IaaS products and services.[44]

One of the primary benefits of cloud computing for the federal government is it is often cheaper for agencies to use cloud computing than maintain the computing resources themselves.[45] Indeed, the federal government spends $90 billion annually on information technology, with 75 percent spent on operating and maintaining current systems.[46] Cloud computing offers agencies the opportunity to convert capital expenses to operational expenses, allowing them to scale their expenses to align with their resource usage and pilot projects without incurring large capital costs. Cloud computing also can increase efficiency and resiliency by allowing agencies to share computing resources. Finally, cloud computing can ensure smaller agencies have access to the highest levels of security they may not otherwise be able to access.

Federal agencies are already experiencing many of the benefits of cloud computing. The U.S. Government Accountability Office (GAO) performed a performance audit from September 2017 to April 2019 of cloud computing in the federal government, finding that 15 of 16 federal agencies it examined had received significant benefits from cloud services.[47] These benefits included cost savings, improved customer service, and improved abilities to collaborate and share information with other government agencies, automate business processes, and offer teleworking opportunities to employees.[48] Specifically, the Department of Labor used cloud services to scale its resources during higher demands for processing, as did DOD, which reported system response times improved from minutes to seconds after migrating to IaaS.[49] In addition, cloud services saved 13 of the examined agencies a combined $291 million between 2014 and 2018. Agencies may have saved even more from leveraging cloud computing because the reported savings only include cloud cost savings or avoidances for projects with life-cycle costs of $1 million or more, and the agencies provided savings data for 16 percent of their cloud investments.[50] Lastly, the agencies frequently reinvested their savings. For example, the U.S. Department of Education used nearly $500,000 in cloud savings from 2018 to modernize its network infrastructure to increase multipath bandwidth and implement software that automatically routes traffic when issues occur.[51] The wide-ranging benefits of cloud computing make it clear that it is in the interest of the government to remove any unnecessary barriers to its adoption.

Federal Investment in Cloud Computing Is Increasing

Due to the benefits, agencies are spending significant funds on cloud computing, thereby increasing the importance of FedRAMP. GAO found that 16 federal agencies spent roughly $1.38 billion on cloud services that had life-cycle costs of $1 million or more in 2017.[52] In addition, the agencies projected they would spend 11 percent of their IT investment on cloud

services in 2019, compared with 9 percent in 2018.[53] Agencies' transition to the cloud will likely continue to increase for several reasons. First, the Office of Management's Cloud First policy requires agency CIOs to use cloud services whenever there is a secure, reliable, and cost-effective option.[54] Second, Congress passed the Modernizing Government Technology Act in 2017, which allows agencies to establish funds to modernize through actions such as transitioning to cloud computing.[55] Third, a proposed stimulus bill to combat the effects of COVID-19, the Health and Economic Recovery Omnibus Emergency Solutions (HEROES) Act, would provide the Technology Modernization Fund $1 billion to respond to coronavirus. At the time of this report, the bill, introduced on May 12, 2020, has passed the U.S. House of Representatives but not the Senate. Nonetheless, the bill passing the House of Representatives suggests some congressional members are willing to provide significant funding to modernize government IT.[56]

THE BENEFITS OF FEDRAMP

FedRAMP has had several beneficial effects on cloud computing use in the government. First, the reuse of authorized systems has helped the government avoid an estimated $285 million in costs.[57] Second, the ability to reuse security packages expedites the adoption of cloud services by federal agencies. For example, using a FedRAMP-approved vendor helped GSA save time and resources because it did not have to a review the vendor's facility.[58] Moreover, 21 of 23 agencies GAO interviewed stated that JAB P-ATOs reduced the time and cost of reviewing cloud services.[59] In addition, FedRAMP can increase a CSP's overall security because it requires providers to implement a set of security controls. By doing so, the security of commercial off-the-shelf cloud solutions improves, which benefits both government and nongovernment customers.[60] Indeed, multiple agencies have reported FedRAMP has improved their security.[61]

The program has also made several attempts to improve since its inception in 2011, many of them successful. For example, the program launched FedRAMP Accelerated in 2016 to reduce the length of time it takes to get a JAB authorization from 12– 24 months to roughly 6 months or less.[62] FedRAMP Accelerated requires CSPs to first work with a 3PAO to obtain a readiness assessment that demonstrates to the PMO that the CSP has the capabilities to receive a P-ATO eventually.[63] The transformation also better defines the roles of JAB and PMO, reducing duplication of their efforts, and incorporated continuous monitoring into the authorization process to improve security assessment.[64] While JAB reviews can still take longer than six months, the authorization time has nonetheless improved. In 2017, the program launched FedRAMP Tailored to make it easier for agencies to adopt SaaS solutions with low-risk profiles.[65] This authorization process is for services such as collaboration and project management tools that do not share personally identifiable information, except for what a person needs in order to log in to a system, such as their username.[66] Services using this path can implement a smaller set of controls compared with systems categorized at the traditional low-impact level, thereby allowing for faster authorization timelines.[67]

FedRAMP has undertaken several other steps to improve as well. For example, GSA's Technology Transformation Services launched an ideation challenge in July 2019 to gather ideas on how to improve FedRAMP, receiving 60 submissions.[68] This challenge led to the creation of agency liaison program that trains individuals to be FedRAMP experts within their respective agencies.[69] More than thirty agencies participate in the program.[70] FedRAMP has also hosted meetups for

small businesses and start-ups, offered in-person training sessions, and created a training platform to educate CSPs and 3PAOs.[71] Finally, GSA partnered with NIST to create the Open Controls Security Assessment Language (OSCAL). The language describes security controls in a standardized and machine-readable format, and enables providers to express their system security plans, which describe how a CSP has implemented the necessary security controls, in a machine-readable format.[72] OSCAL may enable automation in both the documentation and assessment of security controls.[73]

These efforts have improved FedRAMP. For example, the pace of FedRAMP authorizations has increased. Between 2011 and 2014, there were 40 authorizations in total. But in 2018, there were 40 authorizations alone, and 2019 saw the approval of 45 new products.[74] In 2015, it took 13 months on average for a JAB authorization. In 2018, the average JAB authorization took 5.5 months.[75] In 2015, agency authorizations took an average of 15 months. In 2018, the average agency authorization took eight months.[76] The average number of reuses of authorized systems has also increased from three in the first five years of FedRAMP to eight in 2019.[77] More than 150 agencies, including subagencies, are using FedRAMP-authorized services, and nearly 50 are using 10 or more different services.[78]

FEDRAMP AUTHORIZATIONS STILL SLOW, COSTLY, AND INEFFICIENT

Despite its improvements, FedRAMP still has three main drawbacks: the authorization process is lengthy, costly, and does not lead to sufficient reuse of authorizations. Even GSA admits that the FedRAMP authorization "process still takes a significant amount of time."[79] While it can take less than six months for a JAB P-ATO, the JAB only reviews roughly three providers a quarter.[80] For agency ATOs, it takes roughly 6 to 12 months for a CSP to receive an ATO, but it has taken as long as nearly 2 years.[81] For example, it took Virtru, a SaaS provider that creates solutions to help organizations securely share data, 20 months between 2017 and 2019 to receive an ATO from the Federal Communications Commission.[82] The total cost of obtaining an ATO can also be over $500,000.[83] In Virtru's case, the authorization cost $1.6 million, affecting the financial resources the firm had to spend on hiring and product development.[84] Even a gap assessment by a 3PAO, which attempts to identify common issues that prevent a firm from receiving an authorization, can cost as much as $100,000 alone.[85] In addition, the different review strategies of agencies—an agency may force a provider to go through its own government risk and compliance tool in addition to FedRAMP, for example—forces providers to expend additional resources.[86] Finally, annual 3PAO assessments, which FedRAMP requires of agency-authorized systems, can be similar in cost to the original assessment.[87] As such, the cost of FedRAMP can be prohibitively high for many software vendors, forcing some providers to avoid the federal market.[88]

The combination of long timelines and high costs act as a barrier to entry and is particularly burdensome because state and local providers frequently want to use FedRAMP authorized services. As such, providers that do not have the resources to meet FedRAMP requirements can not only be shut out of serving federal customers, but also experience challenges serving state and local government customers. Ultimately, this barrier hinders the ability of federal agencies to leverage cloud computing by making the number of cloud services available to agencies artificially smaller.[89] Consider that roughly half of all authorizations have gone to services built by

or upon the services of 3 firms, and that 36 of 47 surveyed firms stated it was a moderate or significant challenge to implement FedRAMP's requirements.[90]

Another agency issued its own authorization to a service because the FedRAMP authorization process was taking a significant amount of time. These issues undermine the program's main priority, which is ensuring agencies are using secure cloud services.

These barriers also lead to agencies not using FedRAMP to authorize cloud services, even though the program is mandatory for most cloud deployments. For example, GAO published a report in December 2019, that found that 15 of 24 examined agencies did not always use FedRAMP to authorize cloud services. One agency reported using 90 cloud services that were not FedRAMP authorized. The other 14 agencies used 157 cloud services that were not FedRAMP authorized.[91] Two of the agencies stated they could not find FedRAMP authorized providers that met their needs.[92] Another agency issued its own authorization to a service because the FedRAMP authorization process was taking a significant amount of time.[93] These issues undermine the program's main priority, which is ensuring agencies are using secure cloud services.

Why Are Authorizations Slow, Costly, and Inefficient?

Multiple factors contribute to the length and cost of the FedRAMP authorization process. First, the program is understaffed and underfunded. For example, JAB staff frequently have other job duties besides FedRAMP.[94] The PMO office notes that its current funding levels provide enough resources for the JAB to review a up to 12 cloud services a year, which limits the ability of some CSPs to receive a JAB P-ATO, and slows the introduction of innovative services to the government.[95] Furthermore, staffing shortages at agencies also elongate the agency-ATO reviews.[96] In addition, staff turnover, either at the JAB or within agencies, leads to the loss of knowledge of the authorization process and CSPs' services. Consequently, CSPs frequently must re-explain how their services work to new staff.[97] Federal agencies have also reported that it is a challenge to provide the resources to comply with FedRAMP.[98]

Second, many agencies do not trust another agency's ATO. As Rep. Gerry Connolly (D-VA), who serves as chairman of the House Subcommittee on Government Operations, has noted, FedRAMP "continues to suffer from a lack of agency buy-in."[99] Indeed, on average, nearly nine agencies are currently leveraging JAB P-ATOs to provide an ATO, while agencies are currently leveraging agency ATOs less than three times after the initial ATO on average.[100] Some of this difference could stem from agencies procuring services that fit possible niche needs. Nonetheless, the difference suggests that not only do agencies trust JAB P-ATOs significantly more than agency ATOs, but also that agencies may suffer from free-rider incentives, in which they will wait for the JAB to provide a P-ATO before they review a cloud service. This problem also exists to a lesser extent for agency ATOs. Eight agencies have accounted for more than half of the initial authorizations by agencies for cloud services, but 70 agencies—not including subagencies—are using a FedRAMP-authorized cloud service.[101]

Nonetheless, there are likely several reasons for agencies not trusting each other's authorizations, including they have different review processes and security requirements, which leads to some agencies having a higher or lower tolerance for accepting risk.[102] There are also varying levels of FedRAMP expertise within agencies, which can cause a provider to create different strategies for

receiving an ATO at different agencies.[103] If agencies do not leverage existing authorizations, CSPs then have to expend resources at another agency to receive an ATO, rather than the new agency simply reviewing their existing security package and issuing an ATO.[104] FedRAMP has stated that the program is not a market barrier for small businesses because of the ability to reuse authorizations; however, this is only true if agencies have full confidence in using the authorization package of another agency to issue an ATO.[105] Yet, some agencies have even expressed a lack of trust to use an authorization from a different group within its own agency, and questioned the 3PAOs a CSP used to verify and validate security controls.[106]

FedRAMP is still a paperwork-heavy, compliance-focused process.

Third, CSPs often do not know how far along their application is in the certification process.[107] Furthermore, GSA has admitted that a lack of understanding has led to misperceptions by companies about timelines and costs, which can dissuade companies from offering their services to the government.[108] In addition, GSA has acknowledged that the lack of a central forum has led to the perpetuation of outdated stories about FedRAMP, such as the length of authorization processes, which can dissuade agencies and services providers from undertaking the process.[109] The PMO also has limited authority, which hinders its ability to convey how CSPs should implement a control.[110]

Finally, FedRAMP is still a paperwork-heavy, compliance-focused process. Providers have to fill out up to 33 Word documents and Excel spreadsheets, which can total over 1,000 pages, documenting how they have implemented security controls, which can total more than 400.[111] While FedRAMP has a secure repository for agencies to review such documents, relevant parties—such as the CSP, 3PAO, JAB, or agency—email comments and requests about these files back and forth.[112] This process is inefficient, with CSPs often sending the same information to multiple parties.[113] Agencies also frequently fail to correctly fill out required information in the documentation. For example, agencies have struggled to fully describe how they have implemented security controls, including controls listed as their responsibility.[114] Agencies have also failed to fully summarize the testing of security controls and to provide the FedRAMP PMO with cloud authorization letters.[115] Unsurprisingly, agencies have cited managing the complexity of the authorization process as a significant hurdle.[116]

FIXING FEDRAMP

In recent years, several entities have published plans to improve FedRAMP, including the Center for Cybersecurity Policy and Law and the FedRAMP Fast Forward Industry Advocacy Group.[117] These reports include several valuable recommendations, such as expanding the use of "ATO-in-a-day" pilot projects in which agencies have attempted to identify FedRAMP processes to automate and ways to reuse data internally for authorizations.[118] But these reports also highlight that, despite progress, FedRAMP has not solved fundamental issues, such as duplicative processes and a lack of trust between agencies. To overcome these challenges, Rep. Gerry Connolly (D-VA) and Rep. Mark Meadows (R-NC) introduced the "Federal Risk and Authorization Management Program Authorization Act of 2019" (FedRAMP Authorization Act) in July 2019. The bill passed the U.S. House of Representatives in February 2020, and would codify FedRAMP and mandate several beneficial changes.

These changes include providing $20 million a year to JAB and the FedRAMP PMO. Each group sorely needs this funding as they are severely under-resourced.[119] For example, GSA uses the Federal Citizen Services Fund, which it also uses for maintaining websites such as usa.gov and data.gov, to fund the FedRAMP PMO.[120] The significant time commitment FedRAMP requires—FedRAMP's 7 employees attended more than 750 meetings for the program in 2017 alone—indicates that it should have its own, separate funding.[121] This dedicated funding could help in several ways. First, it could help the JAB and PMO hire professional staff. Each could use the extra personnel to speed up reviews. Second, the PMO could also use it to provide additional guidance to relevant parties, develop materials to support the JAB and CSPs in the authorization process, and directly coach CSPs on how to optimize their submissions. The PMO, however, should continue to strive to standardize the authorization process to reduce the amount of coaching that is necessary.

Importantly, the bill also includes measures to increase the reuse of authorizations. For example, it requires agencies to check whether the JAB or another agency has issued a P-ATO or ATO for the cloud product or service before beginning an authorization process. In addition, the act would require, "to the extent practicable," agencies use existing security package documentation to review a cloud system for authorization. The bill strengthens this aspect by stating that the assessment of a cloud system's security controls by JAB or another agency each have a presumption of adequacy for use in agency authorizations.[122]

The FedRAMP Authorization Act would also improve the ability of the program to evolve. The bill creates the Federal Secure Cloud Advisory Committee, which would deliver an annual report to the GSA administrator and Congress that offers recommendations to improve the program. The committee would include up to 15 combined individuals from the public and private sector, including the GSA administrator or their designee, at least five members from the private sector, at least one member each from the Cybersecurity and Infrastructure Security Agency and NIST, at least two officials who serve as chief information security officers at a federal agency, at least one chief procurement officer from an agency, and at least one representative from a 3PAO. The bill also tasks the PMO with creating a process to allow public comment on proposed guidance before it issues such guidance.[123] Both the advisory committee and the comment process would ensure consistent communication with industry, which could help FedRAMP evolve faster.

The bill would also institute several other changes that have potential benefits. These include tasking the PMO with assessing and evaluating ways to automate authorization and continuous-monitoring processes.[124] The automation of either process could reduce the burden of compliance, and increase efficiency. In addition, the bill would increase accountability by requiring the director of the Office of Management and Budget (OMB) to submit an annual report to the U.S. House of Representatives Committee on Oversight and Reform and the Senate's Committee on Homeland Security and Governmental Affairs. The report would provide information on the efficiency and effectiveness of FedRAMP, including data on the reuse of P-ATOs and agency ATOs and the length of the authorization process.[125] Finally, the bill would increase transparency. For example, under the bill, the JAB would need to provide regular updates on the status of cloud services undergoing the assessment and authorization process.[126]

IMPROVING FEDRAMP

Despite numerous provisions in the FedRAMP Authorization Act that would improve FedRAMP, additional reforms are still necessary. We offer several recommendations for both Congress and FedRAMP's administrators. These recommendations can help eliminate redundancies, increase efficiency, and increase agency trust in FedRAMP.

Recommendations for Congress

There are several additional ways Congress can alter the FedRAMP Authorization Act to better meet its goals of increasing the innovation, security, and availability of cloud computing services used in the federal government.[127]

Expand the JAB

Cloud service providers often view a JAB P-ATO as a "gold standard" compared with an agency authorization because the process to obtain the latter can vary from agency to agency.[128] Indeed, nearly every agency GAO surveyed that had experience with the JAB process stated the consistency of JAB officials' review of authorization packages is a beneficial element of FedRAMP.[129] Nonetheless, agency authorizations account for roughly 70 percent of authorizations, partially due to the limited resources of JAB.[130] However, some agencies' lack of trust in reusing authorizations reduces the value of agency ATOs.[131] As such, FedRAMP should strive to scale the JAB authorization process without reducing its effectiveness. The Senate should amend the bill so that it expands the JAB, which currently consists of the CIOs from DOD, DHS, and GSA, to include three additional CIOs from the CIO Council, which is a forum for federal CIOS. In its current state, the bill appropriates "$20,000,000 each year for the FedRAMP Program Management Office and the Joint Authorization Board."[132] Congress should provide the JAB additional funding to accomplish this expansion, including to support the hiring of more dedicated JAB reviewers. Congress should provide the necessary additional funding and clearly delineate the funding each relevant party receives, which would provide it greater oversight into the JAB's operations.

The Senate should amend the FedRAMP Authorization Act so that it expands the JAB, which currently consists of the CIOs from DOD, DHS, and GSA, to include three additional CIOs from the CIO Council, which is a forum for federal CIOS.

The expansion would likely have several benefits. First, it would provide CSPs greater access to a process many consider a gold standard. Indeed, the JAB should not strive to meet its current goal of prioritizing the review of 12 cloud service offerings a year, but to review each offering that meets its requirements, such as demand from six federal customers.[133] Second, it would increase the reuse of P-ATOs by increasing agency trust in the process, and do so by involving more CIOs in the P-ATO process. Third, the increased trust could quicken the speed at which agencies review P-ATOs. Fourth, since an expanded JAB could review more cloud services, the JAB would move closer to becoming a central clearinghouse for authorizations—which could increase standardization—without removing the ability of agencies to authorize a new cloud offering themselves. This expansion is particularly important given that numerous agencies have cited the required time commitment and resources to authorize a service as a challenge.[134] Given the benefits and savings that stem from agencies transitioning to cloud computing, a significant

expansion of the JAB is worthwhile. Indeed, the Congressional Budget Office estimates the FedRAMP Authorization Act would cost $100 million between Fiscal Year 2021 and 2025, which is less than the estimated cost savings 13 agencies realized from transitioning to cloud computing between 2014 and 2018.[135]

Mandate Agencies Receive Exemptions to Not Reuse Authorizations

The FedRAMP Authorization Act would create several ways to increase agency reuse of authorizations, including by establishing a presumption of adequacy of past security assessments for use in new agency authorizations. The bill does not provide a clear way to enforce this provision, however. This lack of enforcement provision is concerning given some agencies' history of disregarding FedRAMP guidelines.[136] The Senate can further increase the use of reauthorizations by altering the bill such that it mandates agencies receive an exemption from the PMO to have a CSP create a separate security package for the agency. In this exemption, agencies would describe why existing security assessments are not adequate for them to conduct a risk review to issue an agency ATO. These exemptions could both highlight agency security practices that may contradict FedRAMP standards and alert the PMO to possible practices it should incorporate into FedRAMP. The PMO should prioritize the review of the exemption requests to ensure the review does not slow down the authorization process.

Expand Technical Expertise of PMO

The FedRAMP Authorization Act rightfully tasks the PMO with evaluating ways to introduce automation into the authorization process. While the PMO has at least one individual focused on strategy, innovation, and technology, it has historically been understaffed.[137] As such, the PMO may lack the expertise to develop and evaluate automation solutions. Furthermore, there are ways to quicken the FedRAMP process besides automation. For example, FedRAMP reformed the JAB P-ATO process because it recognized there was "an overemphasis on documentation." However, CSPs still submit up to 33 Microsoft Word and Excel files during the authorization process.[138] As such, non-automation changes, such as a reduction in the number of required files and the use of a platform wherein all parties could do their work simultaneously, such as providing and responding to comments in real time, could also improve the process.[139] The Senate should amend the FedRAMP Authorization Act to provide funding to the PMO to hire at least two individuals with technical backgrounds whose main job functions are to develop and evaluate innovative solutions for FedRAMP, including automation tools.

Require FedRAMP Liaisons at Each Agency

Too often, the level of support agencies provide to CSPs during the authorization process can vary significantly depending on the agency. Furthermore, it is often unclear to CSPs whom they should contact during the authorization process concerning different issues. FedRAMP has established an agency liaison program to address these and other concerns, and more than 30 agencies participate as of June 2020. The Senate should amend the bill to require that each agency establish an individual as their FedRAMP liaison.[140] The liaisons can coordinate with the PMO, share knowledge about the FedRAMP authorization process within their agency, and ensure tasks needed for authorization are smoothly transferred between the different parties involved. Moreover, the liaisons can act as a conduit to receive and answer all questions between a CSP and agency, thereby reducing duplicative processes.

Require Agencies to Report How They Are Improving Their Authorization Process

The FedRAMP Authorization Act requires the heads of each agency submit to the director of OMB policies for how they will ensure their agencies meet FedRAMP requirements.[141] The Senate should require, along with these policies, each agency to develop plans for how it will improve its FedRAMP authorization process, such as through reducing duplication or increasing communication. For example, the PMO found establishing consistent forms of communication between the PMO and CSPs, such as weekly calls, improved the P-ATO process.[142]

Expand the Number of Metrics Tracked

In its current state, the FedRAMP Authorization Act requires the director of OMB to submit an annual report to Congress that includes data on the "number and characteristics of authorized cloud computing services." To ensure FedRAMP is not acting as a competition barrier for any size of cloud provider, the Senate should change the bill so it explicitly requires that both the JAB and the PMO track more granular authorization metrics, including the time it takes for vendors of different sizes and complexities (SaaS, PaaS, and IaaS) to complete both the JAB and agency authorization processes.[143] This requirement should not be too burdensome, as FedRAMP already reports the dates an authorization process started and the date of authorization for products and services on the FedRAMP Marketplace website.[144] The bill tasks the Federal Secure Cloud Advisory Committee with examining measures to increase the number of authorizations for small businesses, and additional data concerning small businesses' cloud services can help the committee accomplish that task.

Require Agencies and the JAB to Provide Authorization Packages to NIST

The FedRAMP Authorization Act requires that agencies provide a copy of their ATO letters and supplementary information to the FedRAMP PMO. The bill should also mandate that NIST periodically review authorization packages. NIST can analyze these packages to better learn agency needs, which can help it decide which baseline controls to update.[145] The packages can also help NIST identify common weaknesses in how CSPs or agencies are implementing controls.

Recommendations for FedRAMP

There are also a number of steps the administration should take to improve FedRAMP.

Pilot a Tiered Authorization Approach

The FedRAMP authorization process can be long and expensive for CSPs, which can discourage firms from selling their products or services to federal agencies. Moreover, a FedRAMP authorization provides CSPs the opportunity to enter the federal marketplace, not a guarantee of significant business. As such, the risk of entering the FedRAMP process can be prohibitively high for smaller firms.[146]

To address these issues, FedRAMP should pilot tiered authorization processes for JAB P-ATOs and agency ATOs with several willing CSPs and agencies. In this tiered authorization process, CSPs would receive P-ATOs or ATOs for lower impact levels while attempting to receive authorization at a higher impact level. For example, a provider attempting to receive an authorization for a cloud system at the high-impact level could receive an authorization to operate at a moderate level during its authorization process. Alternatively, a CSP undergoing the authorization process for the moderate-impact level could receive an authority to operate at a low level amid its authorization process.

This staged review process would help alleviate some of the adverse effects of protracted and expensive authorization processes by permitting providers to market and sell their services at a lower level while waiting for a higher-level authorization. Moreover, this process removes some of the risk providers take on when entering the FedRAMP process. For example, consider a provider that fails to receive an ATO at the moderate-impact level, but has implemented the necessary controls for the low-impact level. Under a tiered-authorization approach, this provider would still be able to sell its service to the federal government as a low-impact system. Under the current authorization process, no federal agency could use the service at any impact level because the service would not be FedRAMP authorized. Finally, this process could lead to the faster adoption of cloud computing without compromising security. For example, FedRAMP designed the JAB authorization process to ideally take roughly 11 to 12 weeks, including a kickoff (1 week), review (3–4 weeks), remediation (3 weeks), and final review (4 weeks).[147] While some recent JAB authorizations met or exceeded this timeline, others have taken several months longer.[148] By having JAB review and provide a P-ATO in stages, a CSP submitting a cloud system for a high-level authorization could theoretically receive a P-ATO to operate at the moderate level in significantly less time. This change would also allow agencies that do not need a system authorized at the high level to procure the cloud system earlier.

FedRAMP should pilot tiered authorization processes for JAB P-ATOs and agency ATOs with several willing CSPs and agencies.

These changes may require the JAB and agency reviewers to restructure their reviews. Nonetheless, this process could work for several reasons. First, the controls at the low-, moderate-, and high-impact levels build off of each other. For example, the 325 FedRAMP moderate security controls include the 125 controls at the FedRAMP low level.[149] As such, reviewers could analyze whether a CSP has properly implemented security controls in stages, progressing from reviewing the security controls at the low level, and then to the moderate and high levels if necessary. Providers would also remediate vulnerabilities in stages. Second, this process has similarities to the readiness assessment report, which has helped improve the JAB P-ATO process. By requiring CSPs to obtain a readiness assessment report before attempting to enter the JAB review process, FedRAMP has, in effect, already created one stage of a tiered authorization process.[150]

Create Monthly FedRAMP Meetings Between Agency Liaisons

Some agencies' lack of trust in reusing authorizations reduces the value of agency ATOs.[151] As such, FedRAMP should strive to harmonize the agency-authorization process as much as possible. One way to do so is to hold monthly meetings wherein each agency's FedRAMP liaison, JAB reviewers, and other relevant personnel discuss their assessment processes and best practices for implementing controls. These meetings can lead to agencies adopting each other's best practices and facilitate dialogue, which can not only further standardize the FedRAMP authorization process but also increase trust between agencies, which may increase the reuse of agency ATOs.[152]

Create a Mechanism to Ensure Agencies Are Using FedRAMP

A 2019 GAO report recommended OMB "establish a process for monitoring and holding agencies accountable for authorizing cloud services through FedRAMP."[153] GAO had discovered that

numerous agencies were using cloud services that were not authorized through FedRAMP. Nonetheless, the OMB responded that it did not have a mechanism to enforce compliance.[154] The FedRAMP Authorization Act directs OMB to issue guidance to ensure agencies only use FedRAMP-authorized clouds.[155] As such, OMB should create a mechanism to enforce compliance with FedRAMP and hold agencies accountable that do not comply.[156] For example, the OMB director could provide guidance that receiving funds for cloud projects under the Modernizing Government Technology Act, which provides funds to agencies to update aging IT systems through the Technology Modernization Fund, is conditional on only using FedRAMP authorized services.[157] FedRAMP cannot ensure federal agencies are using secure cloud services if agencies do not use the program.

Without the necessary changes and funding, the program risks helping, but also hindering, federal agencies to adopt cloud services.

CONCLUSION

FedRAMP has made significant improvements since its inception in 2011. Nonetheless, the program can still make progress in reducing the time and cost of authorizing cloud services for use by federal agencies. Both the JAB and the FedRAMP PMO should continuously make iterative improvements to the program, such as requiring FedRAMP liaisons at each agency. But the agencies should also use pilot programs to experiment with ways to overhaul how the program currently reviews and authorizes cloud services. Moreover, Congress should pass FedRAMP reform legislation that, among other things, provides the program with the funding it needs to hire more individuals to review cloud services rapidly. Without the necessary changes and funding, the program risks helping, but also hindering, federal agencies to adopt cloud services.

Acknowledgments

The author wishes to thank Daniel Castro and Robert D. Atkinson for providing editorial guidance and feedback on this report. Any errors or omissions are the author's alone.

About the Author

Michael McLaughlin is a research analyst at the Information Technology and Innovation Foundation. He researches and writes about a variety of issues related to information technology and Internet policy, including digital platforms, e-government, and artificial intelligence. Michael graduated from Wake Forest University, where he majored in communication with minors in politics and international affairs and journalism. He received his master's in communication at Stanford University, specializing in data journalism.

About ITIF

The Information Technology and Innovation Foundation (ITIF) is a nonprofit, nonpartisan research and educational institute focusing on the intersection of technological innovation and public policy. Recognized as the world's leading science and technology think tank, ITIF's mission is to formulate and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress.

For more information, visit us at www.itif.org.

ENDNOTES

1. "FedRAMP Accelerated: A Case Study for Change Within Government," FedRAMP, 2017, https://www.fedramp.gov/assets/resources/documents/FedRAMP_Accelerated_A_Case_Study_For_Change_Within_Government.pdf; "Frequently Asked Questions," FedRAMP, accessed March 15, 2020, https://www.fedramp.gov/faqs/.
2. See, for example: "Future of FedRAMP" (Center for Cybersecurity Policy and Law, February 21, 2020), https://static1.squarespace.com/static/5acbb666f407b432519ab15e/t/5e4fd3bf54725e7ce0483940/1582289857151/20-120+Cybersecurity+-+FedRAMP+brochure.pdf.
3. Rep. Brian Fitzpatrick co-sponsors the FedRAMP Authorization Act; FedRAMP Authorization Act H.R. 3941, 116th Cong. (2019); https://www.congress.gov/bill/116th-congress/house-bill/3941/text.
4. FedRAMP Authorization Act H.R. 3941, 116th Cong. (2019), https://www.congress.gov/bill/116th-congress/house-bill/3941/text.
5. "FedRAMP Security Assessment Framework," FedRAMP, November 15, 2017, https://www.fedramp.gov/assets/resources/documents/FedRAMP_Security_Assessment_Framework.pdf.
6. "Agency Guide for FedRAMP Authorizations," FedRAMP, December 7, 2017, https://www.fedramp.gov/assets/resources/documents/Agency_Guide_for_Reuse_of_FedRAMP_Authorizations.pdf; Nate Lord, "What is FISMA Compliance? 2019 FISMA Definition, Requirements, Penalties, and More," Digital Guardian, January 3, 2019, https://digitalguardian.com/blog/what-fisma-compliance-fisma-definition-requirements-penalties-and-more; "What are FISMA Compliance Requirements," SolarWinds, accessed May 5, 2020, https://www.solarwinds.com/federal-government/solution/fisma-compliance-requirements.
7. "FedRAMP Accelerated: A Case Study for Change Within Government," FedRAMP.
8 "Frequently Asked Questions," FedRAMP, accessed March 15, 2020.
9. "FedRAMP Security Assessment Framework," FedRAMP, November 15, 2017; "Frequently Asked Questions," FedRAMP, accessed March 15, 2020.
10. "FedRAMP Security Assessment Framework," FedRAMP, November 15, 2017.
11. "Agency Guide for FedRAMP Authorizations," FedRAMP, December 7, 2017.
12. "FedRAMP Security Assessment Framework," FedRAMP, November 15, 2017.
13. "FedRAMP Jab P-ATO Process," FedRAMP, October 20, 2016, https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/482/2016/10/FedRAMP-JAB-P-ATO-Timeliness-Accuracy-Testing-Requirements-v1-0.pdf; "FedRAMP Readiness Assessments," FedRAMP, accessed March 11, 2020, https://www.fedramp.gov/assets/resources/documents/3PAO_Readiness_Assessment_Report_Guide.pdf; "FedRAMP Security Assessment Framework," FedRAMP, November 15, 2017.
14. "FedRAMP Security Assessment Framework," FedRAMP, November 15, 2017.
15. "JAB Prioritization Criteria and FedRAMP Connect Guidance," FedRAMP, March 26, 2020, https://www.fedramp.gov/assets/resources/documents/CSP_JAB_P-ATO_Prioritization_Criteria_and_Guidance.pdf.
16. "Agency Authorization Playbook," FedRAMP, accessed March 22, 2020, https://www.fedramp.gov/assets/resources/documents/Agency_Authorization_Playbook.pdf.
17. Ibid.
18. "FedRAMP Security Assessment Framework," FedRAMP, November 15, 2017.
19. Ibid.

20. Ibid.
21. "Get Authorized: Joint Authorization Board," FedRAMP, accessed April 1, 2020, https://www.fedramp.gov/jab-authorization/.
22. Ibid.
23. "FedRAMP Accelerated: A Case Study for Change Within Government," FedRAMP.
24. "Agency Guide for FedRAMP Authorizations," FedRAMP, December 7, 2017.
25. Ibid; "Agency Authorization Playbook," FedRAMP, accessed March 22, 2020.
26. "Agency Guide for FedRAMP Authorizations," FedRAMP, December 7, 2017.
27. Cloud Computing Security: Agencies Increased Their Use of the Federal Authorization Program, But Improved Oversight and Implementation Are Needed (Washington, D.C.: Government Accountability Office, December 2019), https://www.gao.gov/products/GAO-20-126.
28. "Future of FedRAMP" (Center for Cybersecurity Policy and Law, February 21, 2020).
29. "FedRAMP Security Assessment Framework," FedRAMP, November 15, 2017.
30. "FedRAMP Accelerated: A Case Study for Change Within Government," FedRAMP; "FedRAMP Security Assessment Framework," FedRAMP, November 15, 2017.
31. "FedRAMP Security Assessment Framework," FedRAMP, November 15, 2017.
32. Tom Risen, "China Suspected in Theft of Federal Employee Records," U.S. News and World Report, June 5, 2015, https://www.usnews.com/news/articles/2015/06/05/china-suspected-in-theft-of-federal-employee-records.
33. Ben Miller, "Tyler Technologies Acquires Socrata," *Government Technology*, April 18, 2018, https://www.govtech.com/biz/Tyler-Technologies-Acquires-Socrata.html.
34. Michael McLaughlin and Daniel Castro, "Most State Unemployment Websites Fail Mobile and Accessibility Tests" (Information Technology and Innovation Foundation, April 15, 2020), https://itif.org/publications/2020/04/15/most-state-unemployment-websites-fail-mobile-and-accessibility-tests.
35. Andrew Westrope, "Rackspace Unveils Program to Speed Up FedRAMP Compliance," Government Technology, May 16, 2019, https://www.govtech.com/biz/Rackspace-Unveils-Program-to-Speed-Up-FedRAMP-Compliance.html#.
36. Ibid.
37. Ibid FedRAMP, FedRAMP Marketplace (Authorized, accessed May 12, 2020), https://marketplace.fedramp.gov/#/products?status=Compliant&sort=productName&serviceModels=SaaS;PaaS,%20SaaS;IaaS,%20SaaS;IaaS,%20PaaS,%20SaaS.
38. Cloud Computing: Agencies have Increased Usage and Realized Benefits, But Cost and Saving Data Need to be Better Tracked (Washington, D.C.: U.S. Government Accountability Office, April 2019), https://www.gao.gov/assets/700/698236.pdf.
39. Hearing on "Cloud Computing: An Overview of the Technology and the Issues Facing American Innovators" Before the Committee on the Judiciary Subcommittee on Intellectual Property, Competition, and the Internet, July 25, 2012 (statement of Daniel Castro, Information Technology and Innovation Foundation), http://www2.itif.org/2012-cloud-computing-open-technology.pdf.
40. Ibid.
41. Ibid.
42. FedRAMP, FedRAMP Marketplace (Authorized, accessed May 29, 2020), https://marketplace.fedramp.gov/#/products?sort=productName&status=Compliant&serviceModels=IaaS,%20PaaS;IaaS,%20PaaS,%20SaaS;PaaS;PaaS,%20SaaS.

43. Hearing on "Cloud Computing: An Overview of the Technology and the Issues Facing American Innovators."
44. FedRAMP, FedRAMP Marketplace (Authorized, accessed May 29 , 2020), https://marketplace.fedramp.gov/#/products?sort=productName&status=Compliant&serviceModels=IaaS,%20PaaS;IaaS,%20PaaS,%20SaaS;IaaS,%20SaaS;IaaS.
45. Cloud Computing: Agencies have Increased Usage and Realized Benefits, But Cost and Saving Data Need to be Better Tracked.
46. Ibid.
47. Ibid.
48. Ibid.
49. Ibid.
50. Ibid.
51. Ibid.
52. Ibid.
53. Ibid.
54. Vivek Kundra, "25 Point Implementation Plan to Reform Federal Information Technology Management" (Washington, D.C.: Office of Management and Budget, December 9, 2010), https://www.dhs.gov/sites/default/files/publications/digital-strategy/25-point-implementation-plan-to-reform-federal-it.pdf; Federal Cloud Computing Strategy (Washington, D.C.: Feb. 8, 2011); Cloud Computing: Agencies have Increased Usage and Realized Benefits, But Cost and Saving Data Need to be Better Tracked.
55. National Defense Authorization Act for Fiscal Year 2018, H.R. 2810, 115th Cong. (2017), https://www.congress.gov/bill/115th-congress/house-bill/2810/text. Cloud Computing: Agencies have Increased Usage and Realized Benefits, But Cost and Saving Data Need to be Better Tracked.
56. The Heroes Act, H.R. 6800, 116th Cong. (2020), https://www.congress.gov/bill/116th-congress/house-bill/6800/text.
57. Lorenzo Winfrey, "FedRAMP Will Drive Transformational Change in Federal Government," Rackspace, July 24, 2019, https://www.rackspace.com/blog/fedramp-transformational-change-in-federal-government.
58. Cloud Computing: Agencies have Increased Usage and Realized Benefits, But Cost and Saving Data Need to be Better Tracked.
59. Cloud Computing Security: Agencies Increased Their Use of the Federal Authorization Program.
60. Will Ackerly, "Testimony to the House Oversight and Government Reform Committee," July 17, 2019, https://oversight.house.gov/sites/democrats.oversight.house.gov/files/2019.07.17%20Ackerly%20Testimony.pdf.
61. Cloud Computing Security: Agencies Increased Their Use of the Federal Authorization Program.
62. "FedRAMP Accelerated: A Case Study for Change Within Government," FedRAMP.
63. Matt Goodrich, "FedRAMP Accelerated," December 29, 2016, https://www.gsa.gov/blog/2016/12/29/fedramp-accelerated.
64. "FedRAMP Accelerated: A Case Study for Change Within Government," FedRAMP.
65. "FedRAMP Tailored Available For Use," FedRAMP, September 28, 2017, https://www.fedramp.gov/fedramp-tailored-available-for-use/.
66. "Launching a FedRAMP Tailored Baseline," FedRAMP, accessed March 25, 2020, https://www.fedramp.gov/launching-a-fedramp-tailored-baseline/.

67. "FedRAMP Tailored for Low-Impact Software- as-a-Service (LI-SaaS)," FedRAMP, accessed March 15, 2020, https://tailored.fedramp.gov/.

68. "Technology Transformation Services Announces FedRAMP Ideation," FedRAMP, news release, July 24, 2019, https://www.gsa.gov/about-us/newsroom/news-releases/technology-transformation-services-announces-fedramp-ideation-challenge; Jory Heckman, "GSA, NIST Look at Automation to Remove FedRAMP Certification Hurdles," Federal News Network, November 19, 2019, https://federalnewsnetwork.com/cloud-computing/2019/11/gsa-nist-look-at-automation-to-remove-fedramp-certification-hurdles/.

69. Brenda Marie Rivers, "FedRAMP Launches Agency Liaison Program to Drive Gov't Knowledge-Sharing," *ExecutiveGov*, June 9, 2020, https://www.executivegov.com/2020/06/fedramp-launches-agency-liaison-program-to-drive-govt-knowledge-sharing.

70. Jason Miller, "FedRAMP Kicks Off New Initiative Thanks to 2019 Ideation Challenge," *Federal News Network*, June 8, 2020, https://federalnewsnetwork.com/reporters-notebook-jason-miller/2020/06/fedramp-kicks-off-fourth-new-initiative-thanks-to-2019-ideation-challenge.

71. "FedRAMP Launches New Training Platform," FedRAMP, June 7, 2018, https://www.fedramp.gov/fedramp-launches-new-training-platform/; Jory Heckman, "GSA, NIST Look at Automation to Remove FedRAMP Certification Hurdles."

72. "FedRAMP Moves to Automate the Authorization Process," FedRAMP, December 17, 2019, https://www.fedramp.gov/FedRAMP-moves-to-automate-the-authorization-process/.

73. Ibid.

74. Mark Rockwell, "Connolly Pushing For New FedRAMP Bill," FCW, July 17, 2019, https://fcw.com/articles/2019/07/17/connolly-fedramp-rockwell.aspx; "GSA, NIST Look at Automation to Remove FedRAMP Certification Hurdles."

75. Hearing on "Federal Risk and Authorization Management Program" Before the House Oversight and Government Reform Committee, 116th Cong. (2019) (statement of John W. Wilmer, Deputy Chief Information Officer for Cybersecurity, Department of Defense), https://docs.house.gov/meetings/GO/GO24/20190717/109809/HHRG-116-GO24-Wstate-WilmerJ-20190717.pdf.

76. Hearing on "Federal Risk and Authorization Management Program" Before the House Oversight and Government Reform Committee, 116th Cong. (2019) (statement of Anil Cheriyan, Deputy Commissioner Federal Acquisition Service And Director Technology Transformation Service, General Services Administration), ://docs.house.gov/meetings/GO/GO24/20190717/109809/HHRG-116-GO24-Wstate-CheriyanA-20190717.pdf.

77. Hearing on "Federal Risk and Authorization Management Program" Before the House Oversight and Government Reform Committee, 116th Cong. (2019) (statement of Anil Cheriyan, Deputy Commissioner Federal Acquisition Service And Director Technology Transformation Service, General Services Administration), ://docs.house.gov/meetings/GO/GO24/20190717/109809/HHRG-116-GO24-Wstate-CheriyanA-20190717.pdf.

78. FedRAMP, FedRAMP Marketplace (Agencies, Products Used, accessed May 12, 2020), https://marketplace.fedramp.gov/#/products?status=Compliant&sort=productName&serviceModels=SaaS;PaaS,%20SaaS;IaaS,%20SaaS;IaaS,%20PaaS,%20SaaS.

79. Hearing on "Federal Risk and Authorization Management Program" Before the House Oversight and Government Reform Committee, 116th Cong. (2019) (statement of Anil Cheriyan, Deputy Commissioner Federal Acquisition Service And Director Technology Transformation Service, General Services Administration), ://docs.house.gov/meetings/GO/GO24/20190717/109809/HHRG-116-GO24-Wstate-CheriyanA-20190717.pdf.

80. "Get Authorized: Joint Authorization Board," FedRAMP, accessed April 1, 2020.

81. Mark Rockwell, "Connolly Pushing For New FedRAMP Bill."

82. Will Ackerly, "Testimony to the House Oversight and Government Reform Committee."
83. Milica Green, "Connolly-Meadows-An Acceleration Lane for FedRAMP," Federal News Network, March 28, 2019, https://federalnewsnetwork.com/commentary/2019/03/connolly-meadows-an-acceleration-lane-for-fedramp/.
84. Will Ackerly, "Testimony to the House Oversight and Government Reform Committee."
85. Andrew Westrope, "Rackspace Unveils Program to Speed Up FedRAMP Compliance."
86. Jory Heckman, "GSA, NIST Look at Automation to Remove FedRAMP Certification Hurdles."
87. Andrew Westrope, "Rackspace Unveils Program to Speed Up FedRAMP Compliance."
88. Ibid.
89. Ibid; "Future of FedRAMP" (Center for Cybersecurity Policy and Law, February 21, 2020).
90. "Future of FedRAMP" (Center for Cybersecurity Policy and Law, February 21, 2020); Cloud Computing Security: Agencies Increased Their Use of the Federal Authorization Program.
91. Cloud Computing Security: Agencies Increased Their Use of the Federal Authorization Program.
92. Ibid.
93. Ibid.
94. "Future of FedRAMP" (Center for Cybersecurity Policy and Law, February 21, 2020).
95. "JAB Prioritization Criteria and FedRAMP Connect Guidance," FedRAMP, March 26, 2020.
96. "Future of FedRAMP" (Center for Cybersecurity Policy and Law, February 21, 2020).
97. Ibid.
98. Cloud Computing Security: Agencies Increased Their Use of the Federal Authorization Program.
99. Carten Cordell, "Connolly Bill Would Compel Agencies to Comply With FedRAMP," FedScoop, July 26, 2018, https://www.fedscoop.com/connolly-bill-compel-agencies-comply-fedramp/.
100. Through email, the PMO directed us that the file to use to calculate the re-use of authorizations was to download the CSV file from the "Authorized" tab on the FedRAMP Marketplace. This CSV denotes which authorizations were initial P-ATOs or agency authorizations, and which authorizations leveraged a P-ATO or agency ATO. We divided the number of leveraged authorizations by the number of initial authorizations or P-ATOs to perform our calculations. Our calculations reflects the current re-use of authorizations, not the total re-use of authorizations. Agencies may revoke or choose not to renew authorizations for a service. As such, our figures will differ from stats referencing the all-time re-use of authorizations. FedRAMP Marketplace (authorized, accessed June 2, 2020), https://marketplace.fedramp.gov/#/products?status=Compliant&sort=productName.
101. Ibid.
102. "Future of FedRAMP" (Center for Cybersecurity Policy and Law, February 21, 2020).
103. Will Ackerly, "Testimony to the House Oversight and Government Reform Committee."
104. "Future of FedRAMP" (Center for Cybersecurity Policy and Law, February 21, 2020).
105. "Impact of FedRAMP for Small Businesses," FedRAMP, January 25, 2018, https://www.fedramp.gov/faqs/; https://www.fedramp.gov/impact-of-fedramp-for-small-businesses/.
106. "Future of FedRAMP" (Center for Cybersecurity Policy and Law, February 21, 2020).
107. Milica Green, "Connolly-Meadows-An Acceleration Lane for FedRAMP."
108. Hearing on "Federal Risk and Authorization Management Program" Before the House Oversight and Government Reform Committee, 116th Cong. (2019) (statement of Anil Cheriyan, Deputy Commissioner Federal Acquisition Service And Director Technology Transformation Service, General

Services Administration), ://docs.house.gov/meetings/GO/GO24/20190717/109809/HHRG-116-GO24-Wstate-CheriyanA-20190717.pdf.

109. Ibid.
110. "Future of FedRAMP" (Center for Cybersecurity Policy and Law, February 21, 2020).
111. Ibid.
112. "Tech Industry's Recommendations For Federal IT Modernization" (Information Technology Industry Council), https://www.itic.org/dotAsset/aa5f716a-2fda-474a-95be-c6778f3783a3.pdf.
113. Ibid.
114. Cloud Computing Security: Agencies Increased Their Use of the Federal Authorization Program.
115. Ibid.
116. Ibid.
117. "Future of FedRAMP" (Center for Cybersecurity Policy and Law, February 21, 2020).
118. Ibid.
119. FedRAMP Authorization Act H.R. 3941, 116th Cong. (2019).
120. "FY 2019 Congressional Justification," U.S. General Services Administration, February 12, 2018, https://www.gsa.gov/cdnstatic/GSA%20FY%202019%20CJ.pdf.
121. David Thornton, "What's Next for FedRAMP? Automation, New Authorizations Later This Year," Federal News Network, June 25, 2018, https://federalnewsnetwork.com/federal-cloud-report/2018/06/whats-next-for-fedramp-automation-new-authorizations-and-more-later-this-year/.
122. FedRAMP Authorization Act H.R. 3941, 116th Cong. (2019).
123. Ibid.
124. Ibid.
125. Ibid.
126. Ibid.
127. Ibid.
128. "Future of FedRAMP" (Center for Cybersecurity Policy and Law, February 21, 2020).
129. Cloud Computing Security: Agencies Increased Their Use of the Federal Authorization Program.
130. "JAB Prioritization Criteria and FedRAMP Connect Guidance," FedRAMP, March 26, 2020.
131. "Future of FedRAMP" (Center for Cybersecurity Policy and Law, February 21, 2020).
132. FedRAMP Authorization Act H.R. 3941, 116th Cong. (2019).
133. "JAB Prioritization Criteria and FedRAMP Connect Guidance," FedRAMP, March 26, 2020.
134. Cloud Computing Security: Agencies Increased Their Use of the Federal Authorization Program.
135. "H.R. 3941, FedRAMP Authorization Act," Congressional Budget Office, February 3, 2020, https://www.cbo.gov/system/files/2020-02/hr3941.pdf; Cloud Computing: Agencies have Increased Usage and Realized Benefits, But Cost and Saving Data Need to be Better Tracked.
136. Cloud Computing Security: Agencies Increased Their Use of the Federal Authorization Program.
137. Jason Miller, "FedRAMP Kicks Off New Initiative Thanks to 2019 Ideation Challenge," *Federal News Network*, June 8, 2020, https://federalnewsnetwork.com/reporters-notebook-jason-miller/2020/06/fedramp-kicks-off-fourth-new-initiative-thanks-to-2019-ideation-challenge.
138. "Future of FedRAMP" (Center for Cybersecurity Policy and Law, February 21, 2020).
139. Milica Green, "Connolly-Meadows-An Acceleration Lane for FedRAMP."

140. Jory Heckman, "GSA, NIST Look at Automation to Remove FedRAMP Certification Hurdles"; John Curran, "GSA Supportive of Report Calling for FedRAMP Modernization Steps," MeriTalk, February 21, 2020, https://www.meritalk.com/articles/gsa-supportive-of-report-calling-for-fedramp-modernization-steps/.
141. FedRAMP Authorization Act H.R. 3941, 116th Cong. (2019).
142. "FedRAMP Accelerated: A Case Study for Change Within Government," FedRAMP.
143. "FedRAMP Accelerated: A Case Study for Change Within Government," FedRAMP.
144. FedRAMP, FedRAMP Marketplace, https://marketplace.fedramp.gov/#/products.
145. Will Ackerly, "Testimony to the House Oversight and Government Reform Committee."
146. Jason Parry, "Overcoming Cloud Adoption Obstacles for Federal Agencies," Nextgov, February 2, 2018, https://www.nextgov.com/ideas/2018/02/overcoming-cloud-adoption-obstacles-federal-agencies/145686/.
147. "Get Authorized: Joint Authorization Board," FedRAMP, accessed April 1, 2020.
148. For example, the JAB authorization process took 10 months for a Google cloud service in 2019; "Google - Google Services (Google Cloud Platform Products and underlying Infrastructure)," FedRAMP Marketplace, accessed May 12, 2020, https://marketplace.fedramp.gov/#/product/google-services-google-cloud-platform-products-and-underlying-infrastructure?sort=authorizations&authorizationType=JAB&impactLevel=High&status=Compliant.
149. FedRAMP Security Controls Baseline, accessed March 25, 2020, https://www.fedramp.gov/documents/.
150. "FedRAMP Readiness Assessments," FedRAMP, accessed June 2, 2020, https://www.fedramp.gov/assets/resources/documents/3PAO_Readiness_Assessment_Report_Guide.pdf.
151. "Future of FedRAMP" (Center for Cybersecurity Policy and Law, February 21, 2020).
152. These meetings can build off the FedRAMP's technical exchange meetings it has begun to implement; Jason Miller, "FedRAMP Kicks Off New Initiative Thanks to 2019 Ideation Challenge," *Federal News Network*, June 8, 2020, https://federalnewsnetwork.com/reporters-notebook-jason-miller/2020/06/fedramp-kicks-off-fourth-new-initiative-thanks-to-2019-ideation-challenge.
153. Cloud Computing Security: Agencies Increased Their Use of the Federal Authorization Program.
154. Ibid.
155. FedRAMP Authorization Act H.R. 3941, 116th Cong. (2019).
156. Cloud Computing Security: Agencies Increased Their Use of the Federal Authorization Program.
157. Chase Gunter, "OMB's User Guide to the MGT Act," FCW, February 6, 2018, https://fcw.com/articles/2018/02/06/mgt-guidance-omb-memo.aspx; "Funding Guidelines," Office of the Federal Chief Information Officer, accessed May 12, 2020, https://policy.cio.gov/modernizing-government-technology/funding/.