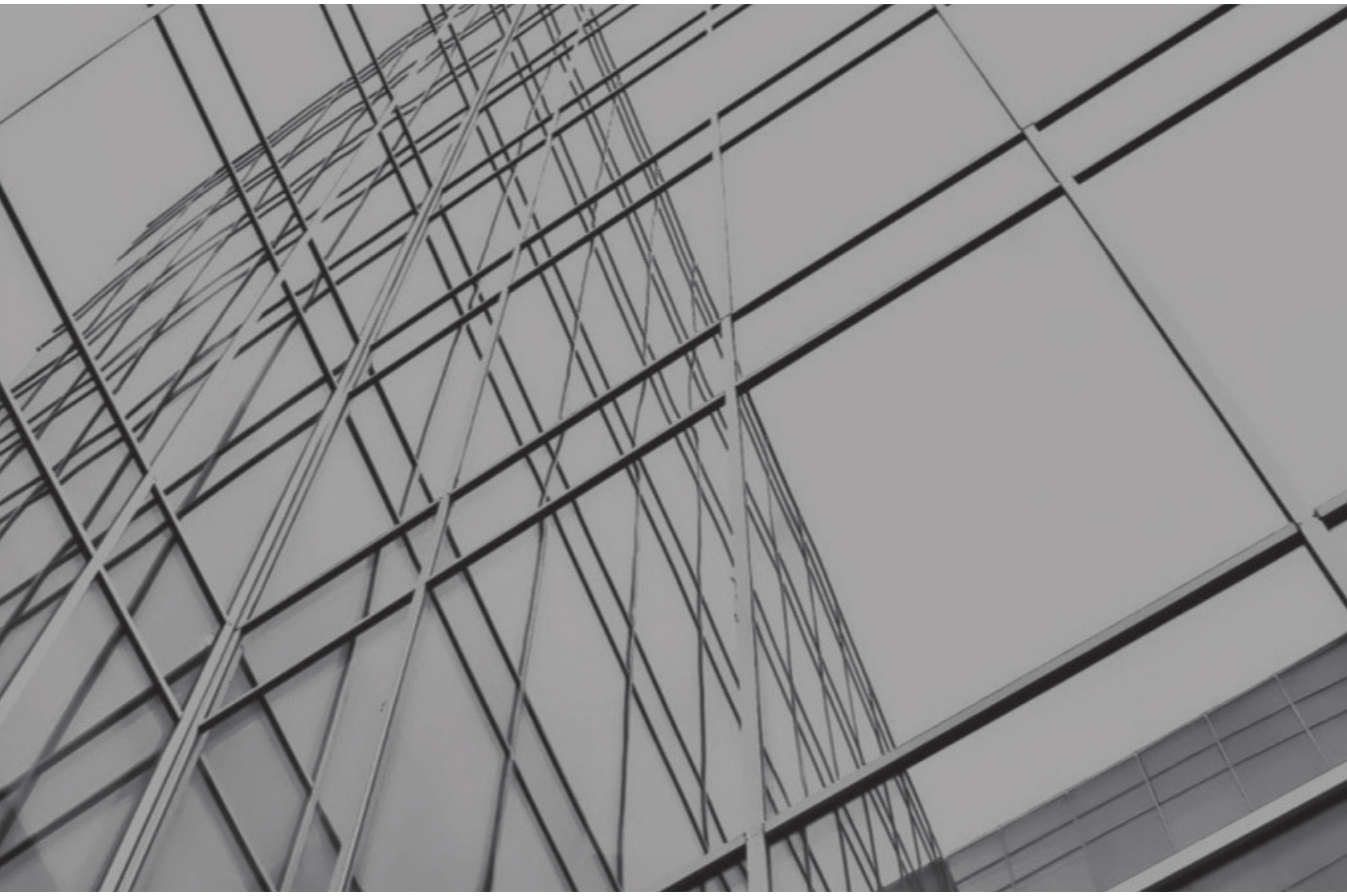
CENTER FOR CYBERSECURITY
POLICY AND LAW



The Future of FedRAMP

February 21, 2020

CONTENTS

EXECUTIVE SUMMARY

Public sector information technology (IT) infrastructure is complex and varied across agency environments. Keeping it updated and ensuring the security and privacy of the increasing amount of sensitive data that travels through and resides within it is a monumental task. Adding to the complexity is the rapid pace of technological advancement, inconsistent funding, evolving global adversaries, shifting federal strategies, and changing legal and regulatory requirements. These issues have helped create an ethos of caution and risk aversion that stymies needed IT modernization efforts and has entrenched a compliance-over-outcome approach to security.

One widely acknowledged pathway to achieving modernization goals is to embrace cloud products and services. To this end, the Federal Risk and Authorization Management Program (FedRAMP) was designed to accelerate the adoption of security cloud solutions through the reuse of assessments and authorizations; improve confidence in the security of cloud solutions and security assessments; achieve consistent security authorizations using a baseline set of agreed-upon standards for cloud product approval within or outside of FedRAMP; ensure the consistent application of existing security practices; and increase automation and near real-time data for continuous monitoring. Additionally, the cloud pathway laid a foundation for a transition to a more modern, risk-based strategy.

While well intended and partially successful, FedRAMP's design is no longer optimized for modern security solutions. It is unsuited to the growth of emerging technologies like the Internet of Things (IoT) and artificial intelligence/machine learning (AI/ML) and is not dynamic enough to incorporate new innovative products. These deficiencies are a result of FedRAMP's limited resourcing and ability to keep pace with agency and cloud service provider (CSP) demand for review and authorization, agencies' limited reuse of authorizations to operate (ATOs), and the compliance-focused, manually driven certification and maintenance process that underpins the interaction between agencies and CSPs. These deficiencies create an opportunity to revise FedRAMP in a manner that reflects a maturation of the government's risk-management approach and improves IT modernization outcomes.

This paper discusses FedRAMP in the context of broader federal government cybersecurity risk management evolution. FedRAMP should continue to evolve into a more dynamic program that is better positioned to serve federal departments and agencies through a streamlined approach to risk management that allows greater access to the innovations happening in the commercial space. The paper summarizes the origins, goals, and evolution of FedRAMP; analyzes the factors that have slowly degraded FedRAMP's efficiency; and offers practical recommendations for modernizing the program.

In an effort to reshape FedRAMP into a risk-based security program that can address contemporary challenges, the Center focuses on the principles of security, scalability, and automation as it makes the following recommendations and associated actions.

Recommendation 1

Redefine federal IT risk management, including FedRAMP, to place continuous, incremental, and automated monitoring at the heart of the process.

- Identify FedRAMP controls that can be automatically assessed for all systems, whether cloud or on-premises, and implement a process for automated certification against these controls.
- Continue efforts to develop fully automated standards for security assessments.
- Update the FedRAMP Security Assessment Framework[1] to make it consistent with the NIST Cybersecurity Framework.
- Develop dashboards for real-time monitoring of government cloud computing environments.

Recommendation 2

Consolidate and standardize the process for risk acceptance across the federal government.

- Create a shared service center or enhance an existing shared service center to consolidate, standardize, and scale the cloud ATO review process.
- Inventory and consolidate existing "ATO-in-a-Day" projects occurring across the federal government to consolidate resources and accelerate adoption of these methodologies.
- Establish a framework for grouping multiple agencies with similar risk profiles to simplify cross-agency acceptance of ATOs.
- Develop and issue additional guidance to provide clarity and direction for reciprocal acceptance of cloud ATOs.

Recommendation 3

Enable the federal government to leverage the full scope of emerging innovation in the cloud computing and information technology markets.

- Develop standard configurations for IT environments and components that can be automatically deployed by IT professionals working across agencies.
- Create and publicize compliance pathways that make it simpler for CSPs with new or updated technology to sell to federal customers.
- Establish and report ATO-related metrics via annual FISMA reporting to provide accountability.
- Study how to accelerate the secure adoption of IoT- and AI-enabled cloud services and software and ensure that compliance requirements do not create unnecessary barriers to innovative solutions.

INTRODUCTION

The scale of the information technology infrastructure that supports the U.S. government is unimaginable to most Americans. Federal civilian departments and agencies alone constitute over 100 organizations that provide a countless range of services, many critical to national security and economic prosperity. They maintain personally identifiable information (PII) and personal healthcare information (PHI) on citizens, and statistical and historical data. Simply put, the U.S. government is one of largest holders of sensitive information in the world today.

Building and maintaining the security and privacy of that information and ensuring mission readiness for technology assets are key drivers across all agencies. However, doing so comes with significant challenges. Frequently impacted by inconsistent funding, evolving global adversaries, and the ever-changing technology landscape, the U.S. government has had its fair share of struggles in keeping its technology up to date. This challenge is further complicated by complex and changing security requirements, set through law or by government agencies, that have resulted in a lack of unified vision and strategy for understanding and managing cybersecurity risk.

Complex systems, critical missions, and concerns over security and privacy have created an IT decision-making process that remains averse to change, even as the federal government seeks to take advantage of technological advancement. This aversion can lead to significant delays in IT modernization efforts and the implementation of innovative security solutions, both of which continue to be a focus across all government departments and agencies. This combination of pressure to modernize and the challenges in doing so often drives agencies into making near-term procurement decisions for technology that adheres to strict, prescriptive, and rapidly outdated security requirements. This is not good for security or for the intended outcome.

To ensure that near-term modernization goals can be achieved and be sustained in the long term, a move toward an informed, risk-based strategy for addressing cybersecurity risks is needed. This strategy should clearly favor modernization and innovation to ensure the government can securely procure and implement modern technologies while enabling measurement and reporting. One clear path to achieving this is through cloud products and services.

Cloud computing emerged early as an important component of IT modernization, and FedRAMP[2] has been an essential enabler of federal cloud adoption. Using standardization, testing, and risk management principles as part of the cloud service procurement process, FedRAMP has demonstrated what a thoughtful and well-run government program can achieve in the foundational areas of security, scalability, and automation.

However, FedRAMP was originally designed around an earlier generation of technology and deployment models that moved at a deliberate, human speed. Furthermore, FedRAMP inherits security controls from a compliance regime designed for an earlier, far more technologically static era, which cannot always be easily adapted to address newer technology and architectures. The cloud market is not static, and government compliance cannot be either.

Moreover, the entrenched continuity and self-reinforcing expectations of the existing laws, policies, practices, and processes mean that incremental program-level adjustments cannot address the fundamental challenges associated with federal adoption of modern information technology and practices, including cloud computing. It is time to revisit and revise the federal risk management processes at a scale that keeps pace with the speed of innovation, by embracing new approaches grounded in the following principles:

- **Security**: Maintain a high standard of security and trust, regardless of any changes to programs now or in the future;
- **Scalability**: Build and maintain a flexible and scalable process to allow for easy adoption of new cloud products, services, and technologies while minimizing unnecessary documentation; and
- **Automation**: Ensure that security controls included in the baselines are continuously monitored through automation in a way that is flexible and adaptable to real organizational risks.

These principles should guide the evolution of risk management for the people, processes, and technology upon which the government depends.

A modern approach to managing risk in the cloud will leverage the automation and scalability inherent in the cloud to enhance security, accelerate IT modernization, and further reduce the workload on both industry and government. This work is not only vital to accelerating the adoption of existing technologies like cloud; it is also pivotal in ensuring that existing compliance regimes are not a barrier to the adoption of emerging technologies like artificial intelligence (AI) and Internet of Things (IoT). Robust government IT is and will continue to be enabled through access to a diverse range of companies — from innovative start-ups to Fortune 100 technology vendors. FedRAMP has been and can continue to be a leader in enabling this access.

METHODOLOGY

In completing the work for this paper, the Center researched and reviewed materials available from both the federal government and private sector CSPs. We interviewed current and former government officials who have been involved in multiple aspects of the FedRAMP program and talked to CSPs of various sizes that have been through and are going through the process. Our recommendations are focused on enhancing FedRAMP in the context of broader federal risk management improvements and focus on high-level guidance and associated actions. In discussions with both the agencies and the CSPs, the Center received several operational and tactical suggestions meant to streamline the existing processes, not all of which are included here, given their more granular nature.

Every effort has been made to incorporate the views of the many stakeholders involved to arrive at a set of recommendations that benefit all.

SECURITY OF THE FEDERAL CLOUD: ORIGINS, GOALS, AND EVOLUTION

ORIGINS

The federal government's traditional approach to managing security and risk has proved to be one of the greatest barriers to cloud adoption. Under the 2014 Federal Information Security Modernization Act (FISMA), agency officials are required to make a deliberate and informed decision about what systems to put into place. OMB Circular A-130 further requires each agency to issue an authority to operate (ATO) for every deployed system. These ATOs must be signed by a senior accountable official or an executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to the organizational operations, assets, or individuals. Although grounded in sound principles, the practical outcome of this approach has meant considerable inconsistency in how agencies have authorized and procured what have often been identical systems.

To help address this inconsistency and streamline the ATO process for cloud services, FedRAMP was authorized in 2011 by the OMB CIO in a memo to agency heads.[3] This was at a time when cloud computing had already achieved significant adoption in the private sector but was still largely untapped within the federal government. Early concerns around keeping sensitive agency information on infrastructure owned and operated by a strictly commercial entity made many nervous about abandoning their on-premises data centers. Nevertheless, many within government saw the potential in moving the right services and information to the cloud in the right way and needed a means to do so that maintained compliance with existing government security requirements.

STRUCTURE AND GOALS

As shown here in *Figure 1*, FedRAMP[4] involves several government agencies and groups, each fulfilling important roles in the authorization process and program management.

1 FedRAMP Program Structure

The FedRAMP Program Management Office (PMO) is responsible for the day to-day operation of the program and helping to set a strategic vision based on input and direction from the Office of Management and Budget (OMB), the National Institute of Standards and Technology (NIST), Congress, and the CIO Council.

One of the key elements of FedRAMP is the Joint Authorization Board (JAB). Comprising representatives (called "reviewers") from the Department of Defense (DoD), the Department of Homeland Security (DHS), and the General Services Administration (GSA), they are the core decision makers of the Provisional Authority to Operate (P-ATO) process. They are responsible for determining what products and services will be reviewed, reviewing evidence, and approving the final authorization at the end of the process. JAB acceptance of a product or service into the process is based largely on perceived demand, following a detailed set of criteria.[5] It is important to note that a P-ATO does not constitute risk acceptance. While an agency can use the P-ATO as a foundation for its own risk acceptance efforts, it is still required to conduct its own internal ATO process, which continues to be a popular option.

Both approaches require an in-depth assessment of the evidence that supports compliance with the set of controls that are required for the specific product or service seeking authorization. This assessment is conducted by a third party assessment organization (3PAO). These are non-government audit organizations accredited by FedRAMP to conduct assessments as part of the authorization process.

The stakeholders in FedRAMP work together to achieve the following goals[6]:

- Accelerate the adoption of security cloud solutions through reuse of assessments and authorizations;
- Improve confidence in the security of cloud solutions and security assessments;
- Achieve consistent security authorizations, using a baseline set of agreed-upon standards for cloud product approval within or outside of FedRAMP;
- Ensure consistent application of existing security practices; and
- Increase automation and near real-time data for continuous monitoring.

EVOLUTION

FedRAMP has succeeded in accelerating cloud adoption across the federal government. As of this writing, FedRAMP Marketplace[7] lists 127 companies with a combined total of 1402 authorizations across 159 agencies.

A cornerstone of federal security, it has been replicated by the Defense Information Security Agency (DISA) to centralize management of DoD information technology and is looked to by state governments seeking to improve their IT security. It has smoothed the pathway for federal adoption of cloud computing and all of the critical technologies that it supports.

Ironically, the very success of FedRAMP makes it an increasing barrier to federal cloud adoption and a source of risk in federal IT modernization. There have long been complaints regarding the time, cost, and complexity of the process of getting authorized. While FedRAMP has made significant improvements, some of these challenges have grown more acute as the number of cloud products and services seeking to support government missions continues to grow.

FedRAMP has done much to create a systematic approach to addressing agency security concerns around the development, implementation, and adoption of secure cloud computing products and services. Today, the government's push to modernize IT infrastructure through cloud adoption, along with its more advanced thinking around risk management, requires an update to the way it secures new systems and environments.

The reality is that the technology and policy landscape under which FedRAMP was originally envisioned and formed has evolved over the last several years. FedRAMP must adapt to this new landscape in order to ensure its continued success.

THE EVOLVING LANDSCAPE

There are three interdependent areas where the technology landscape has been evolving and will continue to evolve at an increasing pace for the foreseeable future. First, cloud computing technology and the associated market continue to see constant innovation and change. Second, technology and approaches to providing IT security — including through the cloud — are changing rapidly. Finally, federal policy around cloud adoption and security authorities and responsibilities continue to grow and shift.

Evolving Cloud Market

The global cloud services market has been growing steadily for many years — not only in scope and scale, but through the successful introduction of new types of services. This is particularly true in the software-as-a-service (SaaS) market, where considerable innovation is always taking place.

The cloud computing/services market is expected to continue to see robust growth. Gartner projects that worldwide public cloud service revenue will increase from $182.4 billion in 2018 to $331.2 billion by 2022.[8] Others project the global cloud computing market will increase from $270 billion in 2018 to $623 billion by 2023.[9]

Widespread growth in the demand and adoption of cloud services in the private sector has been mirrored within the federal government. An analysis of FY 2018 spending marked the eighth consecutive year in which the combined civilian and defense spending on cloud services rose, with every indication that the trend would continue.[10] Bloomberg Government cited a rise in federal cloud contract spending from $2.4 billion in 2015 to $4.4 billion in 2018, and a projected $5.3 billion in 2019.[11] Furthermore, these numbers may actually underrepresent the amount of federal cloud spending. In an April 2019 report to congressional requesters, the Government Accountability Office (GAO) noted that "inconsistent tracking of spending data, along with confusion in interpreting OMB guidance," had likely led to inaccuracies in agency reported spending.[12]

A large part of what will continue to drive this growth is the proliferation of Internet of Things (IoT) devices. IoT is a key factor in the expansion of the cloud services generally, including within the government, as many IoT devices depend on cloud services to support their operation. As a result, the cloud services that support IoT products will need to grow and evolve to support them.

This proliferation has been rapid and increasingly includes products that are not obvious candidates for internet connectivity. The rush to implement connected capabilities into products is illustrated by the jump in global IoT devices from 3.8 billion in 2015 to 7.0 billion in 2018, and projections of roughly 10 billion by 2020.[13] On a more granular level, the number of cellular connected IoT devices rose from roughly 400 million in 2016 to roughly 700 million in 2018, with projections of 3.5 billion by 2023.[14,15]

As with cloud computing, the growth in general IoT use is mirrored within the federal government, albeit to a lesser extent. A 2017 report from the GAO noted that "Many of the federal agencies we reviewed are conducting or funding broad research in IoT-related technologies."[16] Examples include logistics and monitoring programs for the Department of Defense (DoD), smart buildings and telemetrics for the General Services Administration (GSA), smart grid technologies at the Department of Energy (DoE), a smart farm pilot program for the U.S. Department of Agriculture (USDA), and various intelligent transportation systems at the Department of Transportation (DoT).[17]

FedRAMP was not designed to address IoT security directly, but agencies will continue to feel pressure to increase and improve their capabilities through the use of IoT. This in turn will mean that more cloud products and services will need to be authorized.

Another area driving growth is what is broadly referred to as artificial intelligence (AI). AI products and services generally rely on large-scale computing, making the cloud a natural if not essential place for their implementation. Often the ability to leverage AI capabilities is predicated on being able to utilize the cloud services where they are hosted, which may be outside what an agency has determined to be its cloud security boundary. Replicating such services inside that boundary can be cost-prohibitive, leaving innovations that could benefit agency missions inaccessible.

President Trump signed Executive Order (EO) 13859, Maintaining American Leadership in Artificial Intelligence, on February 11, 2019. This EO launched the American AI Initiative, a government-wide strategy to promote and protect United States AI technology and innovation. As part of this strategy, the White House hosted a summit on AI in the government on September 9, 2019 that highlighted the ongoing efforts across the federal government to harness AI to meet its missions. Specifically, GSA's Technology Transformation Service (TTS) created a Center of Excellence (COE) focused on AI technology adoption in federal departments and agencies. As agencies increase the adoption of AI to support their missions, they will likely leverage cloud-based systems and platforms to harness the necessary computing power to drive scalable solutions.

Evolving Cloud Security

As data processing and the underlying technology that supports it have grown more complex, CSPs have been forced to introduce automation into all areas of cloud management and delivery. This in turn has accelerated the development of even more services, creating a loop of innovation, automation, and increasing scale, all while introducing a wider range of capabilities needed to secure all of it.

As a result, security solution companies continue to develop and update products and services that assist enterprises in monitoring and protecting their various cloud environments, as well as the connections between those cloud environments. These cloud-focused security solutions can allow federal agencies to monitor and protect their legacy systems and their new cloud infrastructure and applications by understanding the data and the individuals interacting with the data across on-premises, hybrid, and fully cloud-hosted environments. However, the compliance and documentation mindset on which FedRAMP is based can make implementing innovative solutions difficult or impossible. This is an unintended consequence, but not one that needs to continue.

As part of its own efforts to meet security requirements, the federal government has increasingly looked to leverage government-specific cloud infrastructures. Major CSPs have invested heavily in providing cloud facilities that are isolated from their private sector counterparts. In part, this has been a reaction to the difficulties in meeting government requirements for public cloud procurements, many of which are developed and driven by agencies other than FedRAMP.

The pace at which innovation is occurring across the technology landscape frequently forces companies to develop and get their products and services to market as quickly as possible. Most often, companies begin by designing a product or service for commercial customers and only later look to expand into the U.S. government market. As a result, they find that the security capabilities required by their commercial customers are not adequate for FedRAMP authorization. They discover that design and implementation decisions made during the development of their product or service are now making FedRAMP certification difficult or impossible without significant redesigns.

Evolving Federal Policy

It's important to recognize that the FedRAMP PMO is only one voice among a range of competing incentives, while also bearing the largest burden of implementation for cloud services and having one of the smallest budgets for implementation. Policy changes are needed to ensure that risk management approaches across government are keeping pace with industry best practices and where CSPs are innovating. Therefore, it is necessary to consider where other changes beyond FedRAMP need to take place.

Several primary stakeholders, including the FedRAMP PMO — housed at GSA — and their key agency partners are involved, as shown in *Figure 1*. Coordination with and between these partners is a critical element for FedRAMP, as it both enables the program's success and highlights its dependence on aspects of federal risk management policy over which the PMO has little or no control.

Office of Management and Budget (OMB)

As the primary executive branch component responsible for providing direction to government agencies, OMB is at the center of the policy decisions needed to continue the evolution of risk management approaches, including the use of cloud. To that end, OMB issued its Cloud Smart strategy in 2019.[18] Far more detailed than previous guidance, Cloud Smart amplifies and updates the direction to agencies, in recognition of how much cloud services have expanded and evolved over the last several years. Cloud Smart outlines a series of actions "that constitute a work plan aimed at creating and updating programs, policies, and resources that the whole of Government will use to advance the Cloud Smart agenda." Naturally, FedRAMP is essential to achieving this goal.

As it pertains to security, Cloud Smart says: "Successfully managing cloud adoption [security] risks requires collaboration between agency leadership, mission owners, technology practitioners, and governance bodies. Coordination between information security and privacy programs is necessary to ensure compliance with applicable privacy requirements and for the successful identification and management of risks to individuals when processing personally identifiable information."

This direction reinforces the importance of FedRAMP as a central player in that coordination and determination of compliance. It also demonstrates that informed and flexible policy directives can enhance the government's ability to manage risk and modernize its information technology.

National Institute of Standards and Technology (NIST)

In recent years, the U.S. government has increased its focus on moving away from compliance-based security to a risk-based and continuous monitoring approach that more closely aligns with industry best practices and international standards. In its role as the developer of standards and guidelines for securing agencies systems, NIST has provided the baselines and risk management processes leveraged by FedRAMP since its inception, many of which have not been updated. That said, NIST is an active proponent in evolving the way the government manages cybersecurity risk.

One example of this is the Open Security Controls Assessment Language (OSCAL).[19] OSCAL is a "set of formats expressed in XML, JSON, and YAML" that "provide machine-readable representations of control catalogs, control baselines, system security plans, and assessment plans and results." At its core, OSCAL assists in standardizing the sharing of control information, which in turn greatly enhances the ability to automate assessment and report of security controls. FedRAMP recently announced that it is adopting OSCAL and "expects [it] will offer a number of benefits to streamlining and automating components of the automation process."[20]

Additionally, the Cybersecurity Framework (CSF)[21] is now driving change within government agencies. Developed over several years by government and industry experts from all sectors, the CSF has quickly become a recognized best practice in developing and managing cybersecurity risk management approaches and programs. Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure mandated U.S. government agency use of the CSF for cybersecurity risk management. Within the private sector, the CSF has received wide support and adoption across most sectors, standardizing how all organizations think and communicate about cybersecurity risk.

Adoption of the CSF as a managing framework demonstrates that federal risk management is moving toward a more flexible approach that uses common language and processes to enable consistent, high-level measurement and reporting while still allowing for varying controls at the system level.

Department of Homeland Security

Over the last several years, the federal government has been shifting how it manages enterprise cybersecurity risk toward a more integrated, consistent, and automated approach. One example of this is the Continuous Diagnostics and Mitigation (CDM) program.[22] Through its multiple elements, CDM seeks to:

- Reduce the agency threat surface;
- Increase the visibility of the federal cybersecurity posture;
- Improve federal cybersecurity response capabilities; and
- Streamline Federal Information Security Modernization Act (FISMA) reporting.

It achieves these goals by providing an integrated collection of capabilities that not only protect agencies but result in aggregated views that help to understand the government risk profile.

Additionally, DHS has been given the authority to directly require agencies to act on important cybersecurity issues via Binding Operational Directives (BODs). This has led to an increased need for continuous, near-real-time monitoring and assessment to validate that required changes are being implemented correctly and on time.

While DHS and FedRAMP routinely coordinate, updates to security requirements meant to quickly mitigate threats can sometimes lack the detailed implementation guidance contained in the NIST documents that underpin FedRAMP. This can create a gap between what agencies are expected to do and the detailed information necessary to ensure effective and consistent application of security requirements.

DHS and FedRAMP are also focused on incorporating a threat-based view of risk management into their baseline development process through the .govCAR program.[23] It is hoped that this partnership will yield a more streamlined approach that agencies and the JAB can take when issuing provisional ATO, with an understanding of the most important controls in a given baseline that must be satisfied based on the threat to a given system.

Legislative

The successes and challenges with FedRAMP have not gone unnoticed by Congress. At the time of the release of this paper, Congressman Gerry Connolly, chairman of the Government Operations Subcommittee, and Mark Meadows, ranking member of the Government Operations Subcommittee, introduced and passed the Federal Risk and Authorization Management Program Authorization Action of 2019[24] in the House. (A full discussion of this legislation is beyond the scope of this paper.) However, the simple fact that congressional overseers are looking to improve the program points to both the importance of FedRAMP and the urgency of updating it to account for modern technology.

Challenges

Over the years, the FedRAMP PMO has worked diligently to balance its limited authority and resources against a CSP environment that has grown in scale and capability and a policy landscape that has been in flux. While these efforts have resulted in some improvements, the current system is failing to keep pace with growth and change in commercial capabilities. This is producing a federal cloud ecosystem that is both less diverse and less innovative than the commercial market. While FedRAMP has been used for over 1400 authorizations, nearly half of those authorizations went to services either provided by or built upon services from three companies.[25]

These limitations are the result of three significant challenges with the current system. First, the FedRAMP system lacks the capacity to keep up with both agency and CSP demand for review and authorization. Second, the application of the FedRAMP review process is itself decreasingly standardized across agencies, undermining the ability to reuse authorizations. Finally, the vendors are required to sustain an increasing workload associated with certifying and maintaining an ever-growing list of cloud services for the government. Taken together, this produces a system that is preventing the government from realizing the full benefits of cloud adoption.

The System Lacks the Capacity to Meet Demand

At the most fundamental level, FedRAMP lacks the necessary resources to scale in the way it is being asked to do. There are simply too few people to meet the demand. Many staff, such as those who support the JAB, are doing so in addition to other agency-specific work. For the JAB, this means that approximately three P-ATO[26] packages per quarter can be reviewed. Furthermore, these packages are prioritized based on the JAB's assessment of what is most important to the federal agencies. This prioritization is not itself inappropriate, but it does mean that there are many systems that do not receive a JAB authorization in a timely fashion. Agencies seeking to deploy cloud services without a P-ATO may face implementation delays and/or additional cost and level of effort. This has an outsized impact on smaller or more innovative CSPs, which may have capabilities that are important to a small group of agencies but face significant compliance hurdles that undermine incentives to work with the government.

If not pursuing a P-ATO through the JAB, CSPs can go through the agency ATO process directly. This requires an agency sponsor who takes on the responsibility of reviewing the security package and awarding the ATO, which can then be leveraged by other agencies.

Whether a CSP chooses to take the P-ATO or agency ATO route depends on several factors, including the amount of perceived demand for a specific cloud service and the agency sponsor for the JAB review. Often agency ATOs are easier to pursue because of the working relationship and understanding that CSP may have around an agency requirement or system. However, one agency may not accept an ATO issued by another agency, forcing the CSP to expend more resources if it wants to sell to multiple agencies.

At both the JAB and the agency level, staffing shortages and capability gaps cause slowdowns in authorization reviews. With the demand to assess security at a detailed level for a variety of CSPs, FedRAMP staff and agency IT staff often need additional time to develop the appropriate understanding about a specific application or update to a system to authorize that system. As one CSP put it, between turnover and workforce shortfalls, vendors often spend most of their time helping the assessors understand the original technology, the updates to the technology, and how those updates continue to meet policy and compliance expectations.

Another point often highlighted in our discussions with both CSPs and agencies focused on the ATO process itself. FedRAMP authorizations often move at the speed of bureaucracy. The process requires paper-based documentation of every security control that must be met. And if those controls are not met in the current design, a plan of actions and milestones (POA&M) must be written and tracked by the vendor, the third-party assessor, and the authorizing agency. While FedRAMP does use automation in the Continuous Monitoring process to track system scans, many interviewees noted that increasing automation anywhere in the documentation and review process would create immediate efficiencies. In addition, some CSPs mentioned that innovative security practices must be worked back to NIST standards that are not cloud native, and many assessors are looking for direct compliance versus security outcomes.

As noted previously, we found that the market for FedRAMP-authorized products is skewed toward major CSPs. The small businesses we interviewed noted that they had trouble investing the resources over an extended period without revenue, especially when those same resources could yield more immediate sales in the commercial market.

Agency Application of FedRAMP Is Inconsistent

Risk management across government differs from one agency to another. Each authorizing official (and an agency may have several) must assess his or her threat landscape and make individual risk-based decisions about whether to allow a new system or application into the agency environment. This creates variability across departments and agencies. In several interviews, we heard from agencies that authorizing officials at one agency do not necessarily trust the authorizing processes at another agency, or even across internal organizations within the same agency. In some cases, this was due to lack of trust of specific third-party assessment organizations used in an authorization. In other cases, one authorizing official believed that another agency accepted more risk than he or she was comfortable accepting, which calls into question the value of agency sponsorship as mentioned above. While this is currently supported, and even encouraged, by existing government risk management approaches, it can lead to frustration and confusion for all parties.

Additionally, because agency ATOs are viewed as inconsistent, the JAB P-ATO has become more of a "gold standard." Given the resource limitations of the JAB and FedRAMP PMO, this creates an artificial barrier to the federal market for cloud service providers that either have an agency ATO or are still working through the ATO process.

Vendor Workload to Meet and Maintain Compliance Is Unsustainable

The current authorization documentation process creates significant friction and inefficiencies. Specifically, the FedRAMP documentation process is significantly slowed by its reliance on manual systems and procedures. CSPs are required to submit up to 33 Word and Excel documents that often total over 1,000 pages and 100,000 words. These manual processes can take six months to two years to complete and are ripe for innovative and automated solutions.

This compliance-based process is misaligned with cloud development cycles. Cloud services have development cycles that move quickly, with regular updates and additional features. In many cases, cloud products and services are updated at a near-continuous rate. Complex SaaS applications can receive updates multiple times a day to correct problems that arise in large-scale computing environments. The focus on compliance makes it difficult for agencies to onboard new systems while maintaining an ATO.

Enabling IT Modernization: Recommendations for Modernizing Federal Cloud Security

The federal government needs access to cloud computing technology to modernize and meet its many mission requirements. Unfortunately, the current federal IT security and compliance processes increasingly impede, rather than support, this access. There have long been discussions about how to reform these systems, and while improvements have been made, in the long term incremental adjustments cannot address the fundamental challenges that exist.

The federal government must, instead, reimagine its approaches to security and compliance such that agencies can leverage the speed and scale of modern information technology. This is the only way to keep up with IT innovation and security best practices. It will increase federal access to innovation, encourage small and medium businesses to work with the federal government, and reduce the effort associated with government-specific compliance requirements.

These recommendations are grounded in the following principles:

- **Security**: Maintain a high standard of security and trust, regardless of any changes to programs now or in the future;
- **Scalability**: Build a flexible and scalable process to allow for easy adoption of new cloud products, services, and technologies while minimizing unnecessary documentation; and
- **Automation**: Ensure that security controls included in the baselines are continuously monitored through automation in a way that is flexible and adaptable to actual organizational risks.

Recommendation 1

Redefine federal IT risk management, including FedRAMP, to place continuous, incremental, and automated monitoring at the heart of the process.

Action 1(a): *Identify FedRAMP controls that can be automatically assessed for all systems, whether cloud or on-premises, and implement a process for automated certification against these controls.*

This would introduce consistency across legacy and modern technologies in a way that could facilitate more migrations. Currently, much of the security control review process is done manually. With controls often numbering in the hundreds, production and evaluation of evidence are time consuming, prone to human error, and inconsistent from one review to the next.

Recognizing this, NIST has been exploring how to further codify the risk management process, which could be the first step in developing and implementing automation within FedRAMP.

NIST should coordinate with private sector companies to identify technical and process solutions that could be aligned with the NIST risk management process, SP 800-53 controls, and FedRAMP. However, in addition to resolving any underlying implementation challenges, OMB will still need to determine how automated IT governance might be reconciled with the existing human-centric approach.

Additionally, control baselines must be monitored and updated on a continual basis as changes in the cloud environment occur.

Action 1(b): *Continue efforts to develop fully automated standards for security assessments.*

Automation will be most successful when it can be "tool agnostic" through the introduction of standards such as the Open Security Controls Assessment Language (OSCAL). Once fully realized, OSCAL will form the basis for the automated assessment of a wide range of security controls and provide consistency between vendor implementations. Work to further develop OSCAL and implement it within FedRAMP should continue, and additional avenues for automation should be considered as necessary.

Action 1(c): *Update the FedRAMP Security Assessment Framework*[27] *to be consistent with the NIST Cybersecurity Framework.*

The NIST Cybersecurity Framework has become mandatory for U.S. government agency cybersecurity risk management and has gained considerable support from CSPs in the commercial sector.

Aligning the Security Assessment Framework with the CSF will enable government agencies to use a consistent structure and language for all risk management activities, whether in the cloud or on premises. Additionally, as mentioned above, aligning FedRAMP with the CSF allows commercial entities to tie FedRAMP certification to their broader risk management strategies.

Action 1(d): *Develop dashboards for real-time monitoring of government cloud computing environments.*

The government's use of dashboards has increased over the years as more automated capabilities have been implemented through CDM and other efforts. DHS, GSA, and OMB should incorporate FedRAMP authorizations and continuous monitoring elements into existing dashboards to provide near-real-time assessments of the security posture of government cloud computing environments. It should also mandate integration with these dashboards in standard contract and acquisition clauses.

Recommendation 2

Consolidate and standardize the process for risk acceptance across the federal government.

The administration, through OMB policy, should allow for consolidated risk acceptance on behalf of agencies through targeted shared services. This centralized risk should be cleared, stated, and socialized with the appropriate oversight authorities, including OMB, GAO, and Congress.

OMB and GSA must be positioned to monitor and publicly display the success and value of existing risk acceptance models, including the increased savings in both time and taxpayer dollars when authorization sharing occurs.

Action 2(a): *Create a shared service center or enhance an existing shared service center to consolidate, standardize, and scale the cloud ATO review process.*

A shared service center consolidates expertise on cloud technology and security into a single location that CIOs, program managers, and other IT experts looking to adopt cloud solutions can tap. Combining all this expertise into a single location will help scale federal expertise in cloud computing and provide a resource to help agencies and vendors navigate the FedRAMP process. Additionally, it would create a clear central hub for developing tools and managing efforts, like the "ATO-in-a-Day" initiatives described below, to assist with cloud migration. This would align with recent OMB and GSA work to create centralized mission support capabilities for the federal government,[28] as well as new quality service management organizations (QSMOs).[29]

Action 2(b): *Inventory and consolidate existing "ATO-in-a-Day" projects occurring across the federal government to consolidate resources and accelerate adoption of these methodologies.*

Several agencies have indicated they have worked on projects to streamline their individual ATO processes. These "ATO-in-a-day" projects look for areas to automate and identify data that can be reused internally. These pilot programs need to be monitored closely, inventoried, and promoted across the government as best practices where applicable.

Action 2(c): *Establish a framework for grouping multiple agencies with similar risk profiles to simplify cross agency acceptance of ATOs.*

The government could establish cohorts of agencies that have similar risk profiles and align them to a common, JAB-like process. This builds on the existing ATO reuse model already supported by FedRAMP. Grouping agencies into these risk-based cohorts will foster stronger trust in other agency ATOs. Today, establishing that trust is difficult because agency authorizing officials cannot be certain how trustworthy another agency's ATO process is. This is particularly true when looking at agencies that have much higher security requirements than others. For example, even for non-classified data, it can be challenging for an agency within the intelligence community to fully trust an ATO from an agency within the Department of Commerce, where security requirements are often much lower.

Cohorts reduce this challenge by enabling agencies to establish trust models at the outset and continue to build trust over time, thereby enabling more efficient sharing of ATOs. One grouping that could form a natural cohort could be the JAB itself. By establishing a process for reuse of its own PATOs, the JAB could develop a playbook for establishing trust between agencies and sharing agency ATOs.

Action 2(d): *Develop and issue additional guidance to provide clarity and direction for reciprocal acceptance of cloud ATOs.*

The FedRAMP baselines create a shared taxonomy for conducting security assessments and issuing ATOs. While there are policies enabling agencies to accept ATOs issued by other agencies, issuing further guidance on reciprocal acceptance of ATOs can help to centralize the legal and political risk that agencies feel when considering whether to reuse another agency's ATO.

Recommendation 3

Take steps to enable the federal government to leverage the full scope of emerging innovation in the cloud computing and information technology markets.

Action 3(a): *Develop standard configurations for IT environments and components that can be automatically deployed by IT professionals working across agencies.*

Organizations that are able to reduce complexity across their IT environments have demonstrated that they are better positioned to manage their cybersecurity risk. For common types of deployments (e.g., storage, email), developing, implementing, validating, and enforcing standard configurations and architectures across agencies can significantly accelerate the ATO process.

In coordination with industry, DHS, OMB, and GSA, NIST should consider developing a pilot program, possibly through the National Cybersecurity Center of Excellence (NCCoE), to demonstrate how common configurations and architectures could be established and implemented for common cloud-based service deployments.

Action 3(b): *Create and publicize compliance pathways that make it simpler for CSPs with new or updated technology to sell to federal customers.*

Understanding and addressing FedRAMP requirements sooner in the development life cycle will enable interested companies to release their products and services in a way that will make FedRAMP certification easier.

FedRAMP should continue expanding its outreach and education efforts, particularly targeted to small and medium-sized companies that want to be compliant but may lack internal resources and expertise.

Action 3(c): *Establish and report ATO-related metrics via annual FISMA reporting to provide accountability.*

Improvements to the ATO process more broadly, and the FedRAMP process more specifically, need to be measured and reported on consistently. Without consistent measurement and monitoring, policy makers will have difficulty determining whether changes to FedRAMP are having the desired impact. Additionally, establishing ATO-focused metrics will help OMB and the FedRAMP PMO determine what else can and should be done to improve agency ATO reuse.

Through its authorities, OMB should develop these metrics and incorporate them into the annual FISMA reporting process.

Action 3(d): *Study how to accelerate the secure adoption of IoT and AI-enabled cloud services and software and ensure that compliance requirements do not create unnecessary barriers to innovative solutions.*

As agencies look to leverage new IoT- and AI-enabled cloud services, OMB, DHS, and GSA have an opportunity to define security control requirements and approaches that are flexible. Adoption of these new technologies provides these policy makers with excellent use cases to implement updates to FedRAMP and the federal government's broader cybersecurity risk management practices.

CONCLUSION

Adapting to the ever-changing technology landscape requires the U.S. government to evolve its policies and procedures for understanding and managing cybersecurity risk. As a complex entity comprising hundreds of departments and agencies, the government faces numerous challenges in its efforts to achieve this goal. These challenges include, but are not limited to, resource constraints, unclear authorities, lack of unified vision, and constantly changing requirements.

However, amid these challenges are many examples of successful programs, and the Federal Risk and Authorization Management Program is widely considered to be one of them.

Cloud computing is an important component of the broader government IT modernization efforts, and FedRAMP has been an important enabler of federal cloud adoption. The goals of the FedRAMP process — security, scalability, and automation — are foundational principles of federal IT security, and there is little reason to change them.

Enabling FedRAMP to continue to achieve those goals requires a modern approach to managing risk that can leverage the automation and scalability of the cloud to enhance security, accelerate IT modernization, and further reduce the workload of both industry and government. Robust government IT is enabled through access to a diverse range of companies — from innovative start-ups to Fortune 100 technology vendors — and leverages advances such as IoT and AI.

Incremental or isolated adjustments to existing laws, policies, practices, and processes are insufficient to address the fundamental challenges associated with federal adoption of modern information technology and practices, including cloud computing. While there are specific changes that can be implemented in FedRAMP itself, these must be consistent with, and driven by, a more unified vision and strategy focused on managing risk across the federal government.

Endnotes

1 https://www.fedramp.gov/assets/resources/documents/FedRAMP_Security_Assessment_Framework.pdf
2 https://www.fedramp.gov
3 https://www.fedramp.gov/assets/resources/documents/FedRAMP_Policy_Memo.pdf
4 https://www.fedramp.gov/about/
5 https://www.fedramp.gov/assets/resources/documents/CSP_JAB_P-ATO_Prioritization_Criteria_and_Guidance.pdf
6 https://www.fedramp.gov/about/
7 https://marketplace.fedramp.gov/#/products?status=Compliant&sort=productName
8 https://www.gartner.com/en/newsroom/press-releases/2019-04-02-gartner-forecasts-worldwide-public-cloud-revenue-to-g
9 https://www.reportlinker.com/p05749258/Cloud-Computing-Market-by-Service-Deployment-Model-Organization-Size-Workload-Vertical-And-Region-Global-Forecast-to.html
10 *An Insider's View of Government Cloud.* Bloomberg Government. https://data.bloomberglp.com/bna/sites/3/2019/04/Insiders-View-of-Government-Cloud-1.pdf
11 Ibid
12 *Cloud Computing.* GAO. https://www.gao.gov/assets/700/698236.pdf
13 https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/
14 https://www.ericsson.com/assets/local/mobility-report/documents/2018/ericsson-mobility-report-june-2018.pdf
15 https://www.ericsson.com/en/mobility-report/internet-of-things-forecast
16 https://www.gao.gov/assets/690/686106.pdf
17 https://www.gao.gov/assets/690/686106.pdf
18 https://www.whitehouse.gov/wp-content/uploads/2019/06/Cloud-Strategy.pdf
19 https://pages.nist.gov/OSCAL/
20 https://www.fedramp.gov/FedRAMP-moves-to-automate-the-authorization-process/
21 https://www.nist.gov/cyberframework
22 https://www.dhs.gov/cisa/cdm
23 https://csrc.nist.gov/CSRC/media/Projects/cyber-supply-chain-risk-management/documents/SSCA/Fall_2018/WedPM2.2-STARCAR%20SCRM%20FINAL%20508.pdf
24 https://connolly.house.gov/uploadedfiles/fedramp_authorization_act_of_2019.pdf
25 https://marketplace.fedramp.gov/#/products?sort=productName – Several of the authorizations in this example constituted products that utilized infrastructure or platforms provided by three companies.
26 "A P-ATO means that the JAB has reviewed the cloud service's authorization package and provided a provisional approval for Federal Agencies to leverage when granting an ATO for a cloud system."
27 https://www.fedramp.gov/assets/resources/documents/FedRAMP_Security_Assessment_Framework.pdf
28 https://www.whitehouse.gov/wp-content/uploads/2019/04/M-19-16.pdf
29 https://ussm.gsa.gov/qsmo/