EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

October 27, 2023

DRAFT FOR PUBLIC COMMENT

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: SHALANDA D. YOUNG

SUBJECT: Modernizing the Federal Risk Authorization Management Program (FedRAMP)

The Federal Risk Authorization Management Program, known as FedRAMP, was established by the Office of Management and Budget (OMB) through a December 8, 2011 memorandum from the Federal Chief Information Officer, "Security Authorizations of Information Systems in Cloud Computing Environments,"[1] to safely accelerate the adoption of cloud products and services by Federal agencies, and to help those agencies avoid duplicating effort by offering a consistent and reusable authorization process.

In 2022, recognizing the value that FedRAMP has provided to Federal agencies and to industry, Congress passed the FedRAMP Authorization Act ("Act"). The Act established FedRAMP within the General Services Administration (GSA) and created a FedRAMP Board to provide input and recommendations to the Administrator of GSA.[2] The Act also requires OMB to issue guidance defining the scope of FedRAMP, establishing requirements for the use of the program by Federal agencies, establishing further responsibilities of the FedRAMP Board and the program management office (PMO) at GSA, and generally promoting consistency in the assessment, authorization, and use of secure cloud services by Federal agencies.

As a result, this memorandum rescinds the Federal Chief Information Officer's December 8, 2011 memorandum, and replaces it with an updated vision, scope, and governance structure for the FedRAMP program that is responsive to developments in Federal cybersecurity and substantial changes to the commercial cloud marketplace that have occurred since the program was established.

[1] https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/assets/egov_docs/fedrampmemo.pdf

[2] Pub. L. No. 117-263, § 5921 (2022), *codified in part at* 44 U.S.C. §§ 3607-16.

I. Background

Since its establishment in 2011, FedRAMP has operated by partnering with agencies and third-party assessors to identify appropriate cloud products and services, evaluate those cloud products and services against a common baseline of security controls, and create authorization packages that agency authorizing officials can use to make informed, risk-based, and efficient decisions concerning the use of those cloud products and services.

At the beginning of the FedRAMP program, the Federal Government was focused on securely facilitating agencies' use of commercially available infrastructure as a service (IaaS)—virtualized computing resources that are natively designed to be more scalable and automatable than traditional data center environments. In the years since, the commercial cloud marketplace has grown, especially in the area of software as a service (SaaS)—cloud-based applications made available over the internet. The COVID-19 pandemic only further accelerated the growth of the SaaS market, as shifts in the workplace landscape led more organizations to rely on remote collaboration tools for their workforce and to expand the online services they provide to their customers.

Because Federal agencies require the ability to use more commercial SaaS products and services to meet their enterprise and public-facing needs, the FedRAMP program must continue to change and evolve. While an IaaS provider might offer virtualized computing infrastructure appropriate for general-purpose enterprise uses, SaaS providers typically offer more focused applications. A large agency might rely on only a few IaaS providers to accommodate its custom applications, but could easily benefit from hundreds of different SaaS tools for various collaboration and mission-specific needs. SaaS providers may also target highly tailored use cases that are only relevant to specific sectors and may not be useful to every agency, but which can significantly enhance the effectiveness of the agencies with missions in that sector.

Beyond the changing cloud marketplace, the Federal Government has learned important cybersecurity lessons over the last decade that should be reflected in its approach to cloud security. Keeping a step ahead of adversaries requires the Federal Government to be an early adopter of innovative new approaches to cloud security offered and used by private sector platforms. Federal agencies all have finite resources to dedicate to cybersecurity, and must focus those resources where they matter the most. The use of commercial cloud services by Federal agencies is itself a major cybersecurity benefit, freeing up resources that would otherwise have to be dedicated to operating and maintaining in-house infrastructure.

Similarly, the FedRAMP program must also focus its attention and engagement with industry on the security controls that lead to the greatest reduction of risk to Federal information and agency missions, grounding them in security expertise and real-world threat assessment. Prescribed compliance procedures can help maintain consistency and basic rigor, but it is important to emphasize that FedRAMP must first and foremost be a security program. To that end, FedRAMP must be an expert program that can analyze and validate the security claims of

cloud service providers, while making risk management decisions that will determine the adequacy of a FedRAMP authorization for re-use within the Federal Government.

Strategic changes to the FedRAMP program will ensure that it can enable the Federal Government to safely use the best of the commercial cloud marketplace for years to come.

II. Vision

The purpose of the FedRAMP program is to increase Federal agencies' adoption of and secure use of the commercial cloud, while focusing cloud service providers and agencies on the highest value work and eliminating redundant effort.

To do this, FedRAMP provides a standardized, reusable approach to security assessment and authorization for cloud computing products and services. The FedRAMP program supports broader efforts to reduce the nation's cybersecurity risks, contributing to a more stable technology ecosystem by incentivizing CSPs to make security improvements that protect all of their Federal customers.

The goal of this guidance is to strengthen and enhance the FedRAMP program. FedRAMP has provided significant value to date, but the program must change to meet the needs of Federal agencies and address the scope of the cloud marketplace. The FedRAMP marketplace must scale dramatically to enable Federal agencies to work with many thousands of different cloud-based services that can accelerate key agency operations while allowing agencies to directly manage a smaller IT footprint.

To achieve this, the FedRAMP program has several strategic goals and responsibilities:

- **Lead an information security program grounded in technical expertise and risk management.** FedRAMP is a security program that should focus Federal agencies and cloud providers on the most impactful security features that protect Federal agencies from the most salient threats, in consultation with industry and security experts across the Federal Government. To do this, FedRAMP must be capable of conducting rigorous reviews and identifying weaknesses in the security architecture of cloud providers. At the same time, FedRAMP is a bridge between industry and the Federal Government, and is expected to thoughtfully navigate situations where unthinking adherence to standard agency practices in a commercial environment could lead to unexpected or undesirable security outcomes.
- **Rapidly increase the size of the FedRAMP marketplace by offering multiple authorization structures.** The FedRAMP program has the challenging task of balancing a variety of risk postures across Federal agencies while creating a baseline for the reliability of FedRAMP authorizations that will support the statutory presumption of their adequacy and lead to their reuse at the appropriate FISMA impact level. FedRAMP is expected to create and evolve multiple authorization

structures, beyond those described in this document, that provide different incentives and flexibilities to agencies to achieve these goals.

- **Streamlining processes through automation.** It is essential that FedRAMP establish an automated process for the intake and use of industry standard security assessments and reviews. Automating the intake and processing of machine-readable security documentation and other relevant artifacts will reduce the burden on program participants and increase the speed of implementing cloud solutions in a timely manner.
- **Leverage shared infrastructure between the Federal Government and private sector.** FedRAMP should not incentivize or require commercial cloud providers to create separate, dedicated infrastructure for Federal use, whether through its application of Federal security frameworks or other program operations. The Federal Government benefits most from the investment, security maintenance, and rapid feature development that commercial cloud providers must give to their core products to succeed in the marketplace. Commercial providers should similarly be incentivized to integrate into their core services any improved security practices that emerge from their engagement with FedRAMP, to the benefit of all customers.

Structurally, FedRAMP consists of two parts: a program management office (PMO) and the FedRAMP Board. The PMO, located within GSA and led by a Director, is responsible for providing a security authorization process that meets the needs of Federal agencies, is reasonably navigable for CSPs, and complies with applicable laws and policies, including this memorandum. The FedRAMP Board, composed of Federal technology leaders appointed by OMB, provides input to GSA, establishes guidelines and requirements for security authorizations, and supports and promotes the program within the Federal community.

III. Scope of FedRAMP

The Act charges OMB with establishing the range of cloud computing products and services that may receive authorizations through FedRAMP.[3] Agencies must obtain a FedRAMP authorization when operating an information system within this scope.

Those products and services are: (1) commercially offered cloud products and services (such as Infrastructure-as-a-Service, Platform-as-a-Service, and Software-as-a-Service) that host information systems that are operated by an agency, or on behalf of an agency by a contractor or other organization; and (2) cross-Government shared services[4] that host any information system

[3] *Id.* § 3614(1)(A).

[4] Whether a particular Federally operated service qualifies as a "cross-Government shared service" for these purposes will be determined by the FedRAMP PMO, consistent with any relevant policies or criteria established by the FedRAMP Board.

operated by an agency, or by a contractor of an agency or another organization on behalf of an agency. This scope applies only to information systems that process unclassified information and are not national security systems as defined in 44 U.S.C. § 3552.

Some cloud services are outside the scope of FedRAMP: (1) cloud-based services that do not host information systems operated by an agency or contractor of an agency or another organization on behalf of an agency; (2) services that are offered by a Federal agency but are not a cross-Government shared service.

Examples of excluded cloud-based services that do not host an information system operated by an agency or contractor of an agency or another organization on behalf of an agency include:

1. Ancillary services whose compromise would pose a negligible risk to Federal information or information systems, such as systems that make external measurements or read information from other publicly available services.
2. Publicly available social media or communications platforms governed under Federal agency social media policies, in which Federal employees or support contractors may or may not enter Federal information.
3. Publicly available services that provide commercially available information.

IV. The FedRAMP Authorization Process

The FedRAMP program makes it easier and more efficient for agencies to securely use cloud products and services by issuing FedRAMP "authorizations." A FedRAMP authorization is not an endorsement of a commercial product. However, by certifying that a cloud product or service has completed a FedRAMP authorization process or issuing a provisional authorization to operate, FedRAMP establishes that the security posture of the product or service has been reviewed and is presumptively adequate for use by Federal agencies. FedRAMP was founded on the principle of reducing duplicative work for agencies and companies alike, and bringing a measure of consistency and coherence to what the Federal Government requires from cloud providers. To that end, if a given cloud product or service has a FedRAMP authorization of any kind, the Act requires that agencies must presume the security assessment documented in the authorization package is adequate for their use in issuing an authorization to operate,[5] and that neither additional security controls nor additional assessments of those controls are required.

This presumption of the adequacy of FedRAMP authorizations does not supersede or conflict with the authorities and responsibilities of agency heads under FISMA to make determinations about their security needs. An agency may overcome this presumption if the agency determines that it has a "demonstrable need" for security requirements beyond those

[5] *Id.* § 44 U.S.C. § 3613(e)(1).

reflected in the FedRAMP authorization package,[6] or that the information in the existing package is "wholly or substantially deficient for the purposes of performing an authorization" of a given product or service.[7] The FedRAMP Director remains responsible for deciding whether an agency's additional security needs merit devoting additional FedRAMP resources and conducting additional FedRAMP authorization work to support a revised package. If additional authorization work is conducted and a new authorization is issued, the sponsoring agency must also document in the resulting authorization package the reasons that it found the existing FedRAMP package deficient. However, these instances should be uncommon, in keeping with this policy of presuming the adequacy of FedRAMP authorizations.

For this presumption to be useful, FedRAMP must ensure that its authorizations can be reasonably relied on by multiple agencies, and that they can be tailored to suit the nature of different cloud services and Federal customer needs.

FedRAMP is responsible for defining the processes and criteria that must be met in order for a cloud product or service to receive a FedRAMP authorization.[8] FedRAMP will establish a set of criteria for expediting the authorization of packages submitted by interested agencies with demonstrated mature authorization processes.

FedRAMP is designed to enable use of innovative cloud technologies by Federal agencies in a way that appropriately manages risks. Accordingly, the FedRAMP authorization process should not only require CSPs to demonstrate security capabilities that meet the expectations of Federal agencies but should also recognize the value of newer industry practices that offer improved security and/or compensate for controls that would ordinarily be required. Acting as a bridge between the Federal community and the commercial sector, FedRAMP is responsible for balancing risk and innovation when applying policies governing Federal agency operations, and helping agencies benefit from newer approaches to information security and technology.

To promote reusability while accommodating different use cases within the Federal Government, FedRAMP will support multiple types of FedRAMP authorizations:

1. **A single-agency authorization,** signed by a Federal agency's authorizing official, that indicates that the agency assessed a cloud service's security posture and found it acceptable.

   These authorizations will be designed to enable an agency to safely use a cloud product or service in a manner consistent with that agency's risk tolerances. The

[6] *Id.* § 3613(e)(2)(B).

[7] *Id.* § 3613(b).

[8] 44 U.S.C. § 3609(a)(2).

FedRAMP Director is responsible for ensuring that the authorization can reasonably support reuse by agencies with similar needs.

2. **A joint-agency authorization,** signed by two or more Federal agencies' authorizing officials, that indicates that the agencies assessed a cloud service's security posture and found it acceptable.[9]

   These authorizations will be designed to enable a cohort of agencies with similar needs to pool resources and achieve consensus on an acceptable risk posture for use of the cloud product or service. The FedRAMP Board and FedRAMP Program are encouraged to proactively identify, organize, and support agency cohorts to reduce their effort and expense in conducting joint-agency authorizations. The FedRAMP Director is responsible for ensuring that the authorization can reasonably support reuse by other agencies that would benefit from using the product or service.

3. **A program authorization**, signed by the FedRAMP Director, that indicates that theProgram assessed a cloud service's security posture and found it met FedRAMP requirements and is acceptable for re-use by agency authorizing officials.

   These authorizations are intended to allow the FedRAMP program to enable agencies to use a cloud product or service for which an agency sponsor has not been identified, but for which substantial Federal use could reasonably be expected were it to be authorized.

4. **Any other type of authorization**, designed by the FedRAMP PMO and approved by the FedRAMP Board, to further promote the goals of the FedRAMP program.

The FedRAMP PMO is responsible for ensuring that the types of authorizations described above successfully achieve their goals, and for generally enabling Federal agencies to safely meet their mission needs. The FedRAMP PMO oversees the process for all FedRAMP authorizations, and works with agency program staff and authorizing officials to make necessary risk management decisions. Agency authorizing officials determine acceptable risk for their agency, and the FedRAMP Director determines acceptable risk for what can be called a FedRAMP authorization.

Regardless of the type of authorization, the FedRAMP review process should consistently assess and validate the core security claims made by a cloud provider. FedRAMP reviews are not limited to reviewing documentation, and may direct that intensive, expert-led "red team"

[9] The joint-agency FedRAMP authorization is similar to that of the FedRAMP Joint Authorization Board "provisional ATO" (JAB P-ATO) used under the prior FedRAMP policy structure. However, unlike a JAB P-ATO, multi-agency authorizations can be issued by any group of agencies that works with the FedRAMP Program. Existing JAB P-ATOs at the time of the issuance of this memorandum will be automatically designated as joint-agency FedRAMP authorizations.

assessments be conducted on any cloud provider at any point during or following the authorization process.

Cloud providers are increasingly using complex architectures and encryption schemes to guarantee confidentiality and integrity, and FedRAMP must be able to validate that relevant implementations are reasonable and appear to work as intended. The FedRAMP Director should draw on technical expertise across government and industry as necessary to ensure that appropriate teams can conduct these assessments.

The FedRAMP Board represents the needs of the Federal community and the interests of the FedRAMP program as a whole, and should be responsive to the evolving needs of the Federal community and the changing nature of the cloud ecosystem. The FedRAMP Board is responsible under the Act for establishing and regularly updating requirements and guidelines for security authorizations used in the FedRAMP process.[10] As such, the FedRAMP Board engages with the FedRAMP PMO and its processes as a whole and is not expected to participate in the approval of individual authorization packages.

The authorization process must integrate agile principles and recognize that security is a risk-management process. To achieve this, the FedRAMP program will leverage the use of threat information to prioritize control selection and implementation. The use of threat intelligence, threat analysis, and threat modeling will help agencies better identify the security capabilities necessary to reduce agency susceptibility to a variety of threats, including hostile cyber-attacks, natural disasters, equipment failures, and errors of omission and commission. This process will also apply to other review procedures, including when a provider seeks to modify an existing FedRAMP-authorized service. Summary findings of this analysis will be available to agencies engaged in the FedRAMP authorization process. The FedRAMP Program will update its security baselines to align with a threat-based analysis, produced in collaboration with the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA), that focuses on the application of those controls that address the most salient threats.

Critical to achieving these strategies are the FedRAMP Marketplace and FedRAMP Ready programs. FedRAMP Marketplace shows cloud products and services that are in progress or have completed a FedRAMP authorization. FedRAMP Ready is a status that cloud offerings can obtain that indicates that a readiness assessment has been reviewed and deemed acceptable by the FedRAMP PMO, in accordance with requirements established by the FedRAMP Board. It shows to agencies that an offering is ready to move forward with a full security assessment for a FedRAMP authorization. Products and services that have been through the FedRAMP Ready process are expected to have a faster authorization process.

[10] 44 U.S.C. § 3610(d).

The FedRAMP Marketplace also includes those products and services that have been granted a FedRAMP authorization, as well as products and services that may not have an existing agency customer but have completed the FedRAMP Ready process or other qualifying procedures as determined by FedRAMP. FedRAMP is encouraged to further explore FedRAMP Ready to help on-ramp additional small or disadvantaged businesses who may provide novel and important capabilities, but could face challenges in accessing the Federal marketplace. Similarly, to support a robust marketplace, agencies may in some circumstances require a FedRAMP authorization as condition of contract award, but only if there are an adequate number of vendors to allow for effective competition, or an exception to legal competition requirements applies.[11]

GSA, in consultation with the FedRAMP Board and the Chief Information Officers Council, develops criteria for prioritizing products and services expected to receive a FedRAMP authorization.[12] GSA will ensure that these criteria prioritize products and services based on agency demand, and critical technologies that might otherwise remain unavailable to agencies, while facilitating the goals of this policy, such as automation, shared commercial platforms, and reuse.

To identify more cloud services that could become FedRAMP authorized, and to accelerate their eventual path to being authorized, FedRAMP will provide additional procedures for the issuance of a type of preliminary authorization that would allowFederal agencies to pilot the use of new cloud services that do not yet have a full FedRAMP authorization. Consistent with FedRAMP's policies and procedures, such a preliminary authorization would provide for use of the covered product or service on a trial basis for a limited period of time, not to exceed twelve months, with the goal of more easily supporting a potential FedRAMP authorization.[13]

V. Automation and Efficiency

As part of a technology-forward program optimized for efficiency and consistency, FedRAMP processes should be automated wherever possible.[14] GSA must establish a means of automating FedRAMP security assessments and reviews by December 23, 2023.[15] To ensure that it meets that requirement, FedRAMP should, to the extent feasible, receive all artifacts in the

[11] Inclusion of FedRAMP Authorization as a condition of contract award or use as an evaluation factor should be discussed with the agency acquisition integrated project team (IPT), including appropriate legal representation. Refer to FedRAMP.gov for Frequently Asked Questions regarding acquisition.

[12] 44 U.S.C. § 3609(b)(2).

[13] FedRAMP will provide additional procedures related to this trial process, and agencies are encouraged to coordinate with FedRAMP to ensure that there is no potential gap in service when the trial period concludes.

[14] 44 U.S.C. § 3609(c).

[15] *Id.* § 3609(c)(2).

authorization process and continuous monitoring process as machine-readable data,[16] through application programming interfaces that support predictable and self-service integration between services operated by FedRAMP and by CSPs.

Automation relies on interoperable standards. The FedRAMP PMO will work with OMB, the National Institute of Standards and Technology (NIST), and CISA, as well as private-sector providers of risk and compliance tools, to provide for the submission of security assessment artifacts and continuous monitoring information using machine-readable, standardized data that facilitates interoperability, and to develop and publish relevant standards for that transition. The FedRAMP PMO will also identify additional FedRAMP processes in need of automation to promote efficiency and effectiveness within the program, and facilitate broader access to FedRAMP artifacts for agency partners with a mission need.[17]

Automating the FedRAMP process goes beyond technical implementation to procedural efficiencies as well. To accelerate the adoption of secure cloud computing products and services, FedRAMP must maintain an analysis of what controls can be shared between cloud products and services that rely on an underlying platform or infrastructure offering. FedRAMP will use that analysis to create guidance that streamlines authorizations for cloud services that use FedRAMP-authorized infrastructure or platforms.

Additionally, many existing cloud offerings have implemented or received certifications for external security frameworks. Performing an assessment of such a framework each time a product that uses it goes through the FedRAMP process unnecessarily slows the adoption of such cloud products and services by the Federal Government. Therefore, FedRAMP will establish standards for accepting external cloud security frameworks and certifications, based on its assessment of relevant risks and the needs of Federal agencies. This will include leveraging external security control assessments and evaluations in lieu of newly performed assessments, as well as designating certifications that can serve as a full FedRAMP authorization, especially for lower-risk products and services. FedRAMP may make risk management decisions regarding acceptable controls for certain situations or types of cloud offerings where there are gaps or misalignments between Federal and external security frameworks, weighing whether broader interoperability with industry security processes, reduced burden on providers, or further streamlining of FedRAMP authorizations and processes may justify acceptance of a given level of security risk any. FedRAMP's determinations in this area must align with the guidance and requirements established by the FedRAMP Board.

---

[16] Artifacts in PDF, Word, or similar formats optimized for human readability should not be considered machine-readable data in this context because they will not as effective for reliably automating program processes as data formats optimized for machine-based consumption (such as JSON, XML, and related formats).

[17] Access processes should be streamlined to expand the number individuals who can approve access, as well as streamline and broaden access for those with a need-to-know. This will also be accompanied by expanding the nature and scope of artifacts provided in a machine-readable format, including control inheritance artifacts.

VI. Continuous Monitoring

FedRAMP's continuous monitoring processes should incentivize security through agility, and should enable Federal agencies to use the most current and innovative cloud products and services possible. FedRAMP should seek input from CSPs and develop processes that enable CSPs to maintain an agile deployment lifecycle that does not require advance government approval, while giving the government the visibility and information it needs to maintain ongoing confidence in the FedRAMP-authorized system and to respond timely and appropriately to incidents.

The FedRAMP PMO, in coordination with the Board and CISA, is responsible for establishing a framework for continuous monitoring of cloud services and products, subject to the approval of OMB and DHS. FedRAMP is encouraged to develop a framework that:

- Prioritizes agility of development and deployment by CSPs, to support automation and DevSecOps practices within the cloud ecosystem;
- Calls for advance notice from CSPs of upcoming security-relevant changes to the FedRAMP-authorized cloud product or service without requiring advance approval from the Government;
- Provides CISA technical data to understand risks and to detect threats to agency information and information systems.
- Avoids incentivizing the bifurcation of cloud services into commercially-focused and Government-focused instances. In general, to promote both security and agility, Federal agencies should be using the same infrastructure relied on by the rest of CSPs' customer base.
- Establishes expectations of authorized CSPs regarding incident response procedures, communication and reporting timelines, and other process that help ensure the Government is protected from potential attacks on cloud-based infrastructure.

For all FedRAMP authorized products and services, the FedRAMP PMO will provide a certain standard level of continuous monitoring support to authorizing agencies. The FedRAMP PMO will set this standard level of monitoring support by analyzing and identifying the highest-impact controls for ensuring security of FedRAMP products and services. It will provide recommendations for the supported monitoring levels to the FedRAMP Board for review, feedback, and concurrence. When finalized, FedRAMP PMO will provide the supported monitoring to all agency customers of authorized FedRAMP products and services.

The FedRAMP PMO may conduct a special review of existing FedRAMP authorizations (regardless of authorization type). The FedRAMP Board must approve the special review and establish an expedited deadline for its completion. Once approved, the FedRAMP Director will work with the FedRAMP Board to jointly convene a technical working group consisting of

members from across the Federal Government with relevant expertise. This working group will develop processes and goals tailored to the nature and technical architecture of the cloud provider, and will oversee the review of the cloud provider's authorizations. Within the deadline established by the Board for the review, the working group will conclude its work and produce a report, submitted to the FedRAMP Director and FedRAMP Board, with any recommended changes that should be required of the cloud provider to maintain a FedRAMP authorization.

When the FedRAMP PMO becomes aware of vulnerabilities in a CSP with a FedRAMP authorization, it will provide that information to the CSP and impacted agencies for remediation and establish escalation pathways for vulnerabilities not sufficiently addressed in a timely manner. Escalation pathways may include public notification of unaddressed concerns for potential agency customers. The FedRAMP PMO will develop and maintain procedures for responding to CISA Binding Operational and Emergency Directives,[18] in collaboration with CISA, OMB, and the FedRAMP Board.

To increase integrity and further trust in the FedRAMP program, FedRAMP should leverage government-wide tools and best-practices to enhance its monitoring efforts. Specifically, FedRAMP must ensure that it uses, to the greatest extent possible, CISA's capabilities and shares relevant data and tools for monitoring FedRAMP's products and services.

VII. Roles and Responsibilities

This section details the responsibilities and interactions of the key government stakeholders that make up or interact with FedRAMP. These stakeholders include GSA, the FedRAMP Board, the FedRAMP Technical Advisory Group, NIST, DHS, and Federal agencies. The roles and responsibilities below are intended to identify many of the critical directives of this policy and applicable statutes.

a. The General Services Administration

GSA resources, administers, and operates the FedRAMP program office, and is responsible for the successful implementation of FedRAMP.[19]

In operating FedRAMP, GSA will fulfill a variety of responsibilities, including:

1) Develop and implement the process for FedRAMP authorizations, in consultation with DHS;
2) Grant FedRAMP authorizations consistent with the guidance and direction of the Board, including program authorizations for cloud products and services that meet FedRAMP requirements and threat-based risk analysis;

[18] CISA's Binding Operational and Emergency Directives may be viewed at: https://www.cisa.gov/news-events/directives.

[19] 44 U.S.C. § 3608.

3) Provide a certain standard level of continuous monitoring support for the highest-impact controls of FedRAMP products and services;
4) Develop partnerships with Federal agencies to promote authorizations and reuse, and establish a secure, transparent, and automated process for enabling agency officials' access to artifacts in the FedRAMP repository;
5) Consult with the Federal Secure Cloud Advisory Committee (FSCAC)[20] as appropriate;
6) Proactively engage with the commercial cloud sector, to represent the priorities of the Federal agency community and maintain awareness of contemporary technology and security practices;
7) Establish systems that support automated, machine-readable processing of authorization materials, and drive adoption of relevant standards throughout the cloud ecosystem;
8) Develop guidance, as necessary, for best practices in the procurement of cloud products and services, in coordination with OMB, the CIO Council, and the Chief Acquisition Officers Council;
9) Establish, and submit to the FedRAMP Board for concurrence, metrics that measure agency participation in FedRAMP, the time and quality of each step of the initial FedRAMP authorization process and ongoing interactions with the FedRAMP program, and any other metrics requested by the FedRAMP Board or OMB to measure program health and follow up with agencies as needed; and
10) Position FedRAMP as a central point of contact to the commercial cloud sector for government-wide communications or requests for information concerning commercial cloud providers used by Federal agencies.

b. The FedRAMP Board

The FedRAMP Board consists of up to seven senior officials or experts from agencies that are appointed by OMB in consultation with GSA.[21] The Board must include at least one representative from each of GSA, DHS, and the Department of Defense, and will include representation from other agencies as determined by OMB. The FedRAMP Board members must possess technical expertise in cloud, cyber, privacy, risk management, and other competencies identified by OMB, in consultation with GSA.[22] OMB may elect to adjust the board membership over time, and the membership will be documented in the FedRAMP Charter maintained by GSA. OMB, through the Federal Chief Information Officer, will participate in FedRAMP Board meetings to provide oversight and and guidance, and the

[20] The Federal Secure Cloud Advisory Committee is established in accordance with the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, as codified at 44 U.S.C. § 3616.

[21] 44 U.S.C. § 3610(b).

[22] *Id.* § 3610(c).

Office of the National Cyber Director may attend Board meetings as appropriate to assist in the coordination of FedRAMP activities with national cyber policy and strategy. As a body intended to represent the entire participating Federal community, the FedRAMP Board should, in general, endeavor to maintain consensus among its members when making decisions. To ensure FedRAMP's effectiveness and efficiency, however, the Board must be able to reach final resolutions even when consensus is unattainable. Accordingly, it is the Board's responsibility to adopt internal operating procedures under which final decisions will be made even in the absence of unanimous support from its members.

As provided in the Act, the Board will:

1) Provide input and recommendations to GSA regarding the requirements and guidelines for, and the prioritization of, security assessments of cloud computing products and services;
2) In consultation with GSA, serve as a resource for best practices to accelerate the process for obtaining a FedRAMP authorization;
3) Establish requirements and guidelines for security assessments of cloud computing services, consistent with standards defined by the National Institute of Standards and Technology, to be used in the determination of a FedRAMP authorization;
4) Establish and regularly update requirements and guidance for security authorizations of cloud computing products and services, including government-wide shared services, consistent with OMB policy and NIST standards and guidelines, to be used in the determination of FedRAMP authorizations;
5) Monitor and oversee, to the greatest extent practicable, the processes and procedures by which agencies determine and validate requirements for a FedRAMP authorization, including periodic review of agency determinations that existing assessments in the FedRAMP repository were not sufficient for the purpose of performing an authorization;
6) Ensure consistency and transparency between agencies and CSPs in a manner that minimizes confusion and engenders trust; and
7) Perform other roles and responsibilities as assigned by OMB, acting through the Federal Chief Information Officer, with the concurrence of the FedRAMP PMO at GSA.

As agreed by OMB and GSA, the Board will also provide input to GSA regarding the establishment of metrics reflecting the time and quality of the assessments necessary for completion of a FedRAMP authorization.

c. Technical Advisory Group

OMB will establish a Technical Advisory Group (TAG) to provide additional subject matter expertise to FedRAMP and advise on the technical, strategic, and operational direction of the

program. The goal of the TAG is to provide additional avenues for input across the Federal community into the functioning of FedRAMP and serve as an independent source for technical and programmatic best practices and insight.

The TAG will comprise up to six technical experts in cloud technologies, cybersecurity, privacy, risk management, digital service delivery, and other competencies as identified by GSA, with OMB concurrence. TAG members will be Federal employees. The FedRAMP PMO will provide operational support for the functions of the TAG.

The TAG will:

1) Provide recommendations on best practices in continuous monitoring of cloud services and establishing control criteria.
2) Provide advice on issues that arise during the process of performing risk assessments and technical reviews of authorization packages.
3) Advise on other issues as requested by the FedRAMP Director or FedRAMP Board.

d. Agencies

To further strengthen the FedRAMP program, each agency must:

1) Upon issuance of an agency authorization to operate based on a FedRAMP authorization, provide a copy of the authorization-to-operate letter and any relevant supplementary information to the FedRAMP PMO, including configuration information as applicable;
2) Ensure authorization package materials are provided to the FedRAMP PMO using machine-readable and interoperable formats, in accordance with any applicable guidance from the FedRAMP program;
3) Ensure that agency system-inventory tools can ingest machine readable authorization artifacts;
4) Provide data and information concerning how they are meeting relevant security metrics, in accordance with OMB guidance; and
5) Ensure that relevant contracts include the FedRAMP security authorization requirements with which the contractor must comply.

e. Department of Commerce

NIST, within the Department of Commerce, is responsible for developing and maintaining standards and guidelines to support implementation of risk management programs to meet the requirements of FISMA. In doing so, NIST has an essential role in the FedRAMP process.

NIST will:

1) In coordination with OMB and CISA, review the underlying NIST standards and guidelines used by FedRAMP to identify and assess the provenance of the software in cloud services and products;
2) Assess and update standards and guidelines, as determined necessary, to keep pace with the evolving technology landscape and support the continued evolution of FedRAMP;
3) Monitor and review private sector information security practices to understand potential application; and
4) Develop and maintain a machine-readable data standard to support automation of security assessments and continuous monitoring, as well as the automation of other artifacts or processes required by the Risk Management Framework for Information Systems and Organizations.[23]

VIII. Industry Engagement

FedRAMP is a bridge between the Federal community and the commercial cloud marketplace. The FedRAMP program makes it easier for agencies to obtain what they need from the commercial ecosystem and accelerate mission operations. At the same time, FedRAMP makes it more feasible for commercial providers to satisfy similar needs across the Federal Government in a consistent and streamlined way.

To further the program's goals, GSA and the FedRAMP Board should engage with industry, through the FSCAC and other mechanisms as appropriate, to maintain a current understanding of industry technologies and practices, to understand where the FedRAMP program could improve its policies or operations, and to otherwise build a strong working relationship between the commercial cloud sector and the Federal community.

The FedRAMP PMO and Board should continue to seek feedback from industry on how to increase agency reuse of FedRAMP authorizations, drive more authorizations of small or disadvantaged businesses, and reduce the burden and cost of the FedRAMP authorization process for both CSPs and Federal agencies.

Additionally, the FedRAMP PMO and Board should proactively work to convene industry to convey the emerging cybersecurity priorities and needs of the Federal Government as an enterprise, and discuss potential solutions.

It is inefficient for CSPs to report the same information repeatedly to each Federal agency customer they serve. The FedRAMP PMO is positioned to act as a central point of contact when the Federal Government needs to gather information about cloud products and services used by agencies. Such needs may flow from OMB policies, CISA Binding Operational or Emergency Directives, or other government-wide directives or initiatives that require the collection of cloud security information.

[23] National Institute of Standards and Technology Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*.

IX. Implementation

Within 90 days of issuance of this memorandum, OMB will appoint an initial slate of members of the FedRAMP Board. The Board must, once constituted, approve a charter.

Within 90 days of issuance of this memorandum and annually upon request, GSA will submit a plan, approved by the GSA Administrator, to OMB, detailing program activities, including staffing plans and budget information, for implementing the requirements in this memorandum. The plan will include a timeline and strategy to bring any pending authorizations or existing FedRAMP initiatives into conformance with the Authorization Act and this memorandum.

Within 180 days of issuance of this memorandum, each agency must issue or update agency-wide policy that aligns with the requirements of this memorandum. This agency policy must promote the use of cloud computing products and services that meet FedRAMP security requirements and other risk-based performance requirements as determined by OMB, in consultation with GSA and CISA.

Within 180 days of issuance of this memorandum, GSA will update FedRAMP's continuous monitoring processes and associated documentation to reflect the principles in this memorandum.

Within one year of the issuance of this memorandum, GSA will produce a plan, approved by the FedRAMP Board and developed in consultation with industry and potentially impacted cloud providers, to structure FedRAMP to encourage the transition of Federal agencies away from the use of government-specific cloud infrastructure.

The FedRAMP Authorization Act requires GSA to establish a means for the automation of security assessments and reviews. Within 18 months of the issuance of this memorandum, GSA will build on this work so as to receive FedRAMP authorization and continuous monitoring artifacts exclusively through automated, machine-readable means.

X. Rescissions

This memorandum rescinds "Security Authorization of Information Systems in Cloud Computing," issued by the Federal Chief Information Officer on December 8, 2011.

XI. Policy and Program Implementation Assistance

Questions about this memorandum should be addressed to the OMB Office of the Federal Chief Information Officer via email: ofcio@omb.eop.gov.