# MITRE’s Response to the OMB RFI on FedRAMP

## December 22, 2023

For additional information about this response, please contact:

Duane Blackburn
Center for Data-Driven Policy
The MITRE Corporation
7596 Colshire Drive
McLean, VA 22102-7539

policy@mitre.org
(434) 964-5023

# About MITRE

MITRE is a not-for-profit company that works in the public interest to tackle difficult problems that challenge the safety, stability, security, and well-being of our nation. We operate multiple federally funded research and development centers (FFRDCs), participate in public-private partnerships across national security and civilian agency missions, and maintain an independent technology research program in areas such as artificial intelligence, intuitive data science, quantum information science, health informatics, policy and economic expertise, trustworthy autonomy, cyber threat sharing, and cyber resilience. MITRE's ~10,000 employees work in the public interest to solve problems for a safer world, with scientific integrity being fundamental to our existence. We are prohibited from lobbying, do not develop or sell products, have no owners or shareholders, and do not compete with industry—allowing MITRE's efforts to be truly objective and data-driven. Our multidisciplinary teams (including engineers, scientists, data analysts, organizational change specialists, policy professionals, and more) are thus free to dig into problems from all angles, with no political or commercial pressures to influence our decision making, technical findings, or policy recommendations.

MITRE has an extensive history of assisting federal agencies in planning and adopting secure cloud solutions to enhance mission delivery. Our work encompasses certification processes like the Federal Risk Authorization Management Program (FedRAMP) and we developed the Enterprise Cloud Adoption Framework[1] (ECAF), a comprehensive tool designed to aid executives and technology leaders in all facets of cloud adoption projects. The ECAF covers all dimensions of cloud adoption, from the application to the enterprise level, integrating policy, mission, and technology considerations. The General Services Administration (GSA) cites this framework as a best practice, and it has received international recognition.

In response to recent significant cyber breaches on government information technology (IT) infrastructure, often orchestrated by state actors, MITRE has also recently established the Cloud Safe Task Force. This task force, formed in collaboration with the Cloud Security Alliance (CSA), the Advanced Technology Academic Research Center, and the IT Acquisition Advisory Council, aims to address the exposed critical cyber resilience deficiencies, particularly in certification processes and known vulnerabilities. The task force's goal is to align industry and government efforts in developing a unified response, ensuring the security of our nation's crucial digital infrastructure against relentless cyber threats. The inaugural meeting of the task force, held on December 4, 2023, saw participation from both government and industry. In addition to our own insights, MITRE leveraged recommendations and discussions from community members in this meeting to craft this response.

# Introduction and Overarching Recommendations

MITRE has thoroughly reviewed OMB's draft FedRAMP memorandum with keen interest. We believe there are ample opportunities to strengthen this program by improving both (1) the government's governance and oversight of FedRAMP and (2) industry's accountability. The key

[1] K. Warren and R. Sabetto. Enterprise Cloud Adoption Framework Briefing. 2022. MITRE, https://www.mitre.org/sites/default/files/2022-05/pr-22-0888-enterprise-cloud-adoption-framework-ecaf-version-2.pdf.

points of our response are outlined below, and we recommend that OMB explicitly address these in their final memorandum. Detailed comments on the draft will follow these highlights.

**Government Governance and Oversight.** The FedRAMP program needs the support and backing of key government cybersecurity leaders. The Director of the Office of the National Cybersecurity Director (ONCD) and the Federal Chief Information Officer (CIO) should have a more formal role on the FedRAMP Board as opposed to the optional role currently stated in the draft memorandum. These leaders can also address government-wide topics more successfully, like coordination and reciprocity across other cloud certification processes.

**Industry Accountability.** The FedRAMP program needs to consider incentives for industry to discover, prevent, and disclose threats and vulnerabilities to their systems and services. These incentives could include a streamlined reauthorization process when updates are made to already certified offerings. Incentives should also be considered to encourage cloud providers to implement the zero trust principles already required within the federal government.

# Detailed Comments on the Draft

This section begins by providing expanded discussion of MITRE's overarching recommendations, followed by additional comments for OMB to consider.

## Expanded Discussion of Overarching Recommendations

**Incentivize cloud service providers (CSPs) to proactively discover, prevent, and disclose threats** and vulnerabilities to their own systems and services, and to promptly remediate those threats.

Given the profit-driven nature of CSPs, new cloud capabilities and services are often developed and introduced before comprehensive cybersecurity measures are implemented. To counteract this, U.S. government acquisition programs could be designed to incentivize CSPs to prioritize vulnerability discovery and remediation efforts. Financial incentives, akin to award fee programs, could be linked to the success of CSPs' risk management initiatives.

Our cyber adversaries employ teams of attackers that tirelessly work to discover and exploit U.S. cyber deficiencies, resulting in an asymmetric battleground. A solution is needed to rebalance the battle space. One example, Bug Bounty programs, has proven relatively successful in discovering vulnerabilities in public-facing IT systems. Both industry and government have effectively implemented Bug Bounty programs, such as the DoD's "Hack the Pentagon," to encourage vulnerability discovery and disclosure.

Typically, U.S. cloud consumers are not informed when CSP systems are compromised. Implementing a CSP notification system, such as a ThreatCon status board, would greatly assist in enabling defensive responses by consumers. While incentivizing such real-time reporting may pose challenges, it is crucial for fostering a more proactive and responsive cybersecurity environment.

The issue of a cloud provider being unable or unwilling to rectify a problem that invalidates its FedRAMP certification also needs to be addressed. The last bullet point on page 11 assumes cooperative cloud partners and a business case for investing in fixes, which represents an ideal though atypical scenario. Regarding the bullet points on page 11, there are several aspects to consider: 1) changes that introduce new issues, such as controls disappearing or functioning differently; 2) changes that alter the default baseline, particularly when something becomes optional and the default is set to "off" instead of "failing secure" on upgrade; and 3) a consistent lack of clarity on instances where services require additional and/or specific actions not otherwise included in the Customer Responsibility Matrix (CRM) for the customer to maintain security/compliance. An example of the latter is a service change that results in data being sent to a non-compliant commercial cloud location for back-end processing, rather than being processed within the local tenant. This change brings performance improvements, cost reduction, and enhanced capability, but also an undisclosed (or stealth-disclosed) impact on compliance/data security. A mechanism should be established for holding CSPs accountable or imposing consequences to encourage CSPs to avoid hidden issues that customers must discover and resolve themselves.

## Encourage CSPs to implement Zero Trust Architecture (ZTA) and cyber resiliency capabilities for securing their own service elements.

On page 4, the memorandum's vision statement emphasizes the need to leverage shared cloud infrastructure for use by commercial and federal organizations. Consequently, this plan should promote the integration of security practices based on a zero trust approach to cloud security into core services of agencies and commercial providers. The memorandum should also reference the initiatives detailed in OMB M-22-09, "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles."[2]

In response to Executive Order 14028[3] and NSM-8,[4] solutions involving the application of zero trust (ZT) security principles are rapidly evolving for U.S. government IT systems, with the cloud being considered an enabler for adoption. While the government is quickly adopting ZTA capabilities and the CSP industry has been successful in providing capabilities and services for government uptake, there is limited evidence to suggest that the CSP industry is also adopting ZTA solutions. FedRAMP and NIST could collaborate to develop or revise industry standards to encourage ZTA capability and practice adoption by CSPs. These standards could function similarly to those established for NIST SP 800-171[5] to drive Cybersecurity Maturity Model Certification by the Defense Industrial Base and government contractors handling sensitive government information.

Cyber resiliency is often perceived as merely an availability issue addressed by implementing system redundancy or disaster recovery methods. However, it encompasses much more and

[2] S. Young. Moving the U.S. Government Toward Zero Trust Cybersecurity Principles. 2022. Office of Management & Budget, https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

[3] Executive Order on Improving the Nation's Cybersecurity. 2021. The White House, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/. Last accessed December 12, 2023.

[4] National Security Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems. 2022. The White House, https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/. Last accessed December 12, 2023.

[5] NIST SP 800-171 Rev. 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. 2021. National Institute of Standards and Technology, https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final. Last accessed December 12, 2023.

complements ZT principles. Cyber resilient systems engineering practices are described in NIST 800-160v2r1.[6] The publicly available MITRE CREF Navigator[7] can be applied to facilitate association of cyber resilience techniques to NIST SP 800-53[8] security controls.

For FedRAMP to promote and incentivize the adoption of ZT principles and cyber resilient systems engineering, security control requirements and/or baselines may need to be revised or expanded to ensure that security techniques are addressed during assessment. While the DoD has developed a ZT Controls Overlay, we advise developing both ZT- and resilience-focused controls overlays at the general federal level.

CSPs provide infrastructure and services that often require signification customer configuration. Misconfiguration of cloud security controls is frequently cited as one of the leading causes of security breaches in the cloud. FedRAMP should incentivize CSPs to adopt stronger security controls by default and disallow weaker configurations. For example, all storage should have encryption enabled by default with automatic key rotation, and customers should be allowed to enable further encryption as required.

On page 8, the memorandum mentions identifying 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. Incorporating resilience would help reduce an agency's susceptibility to natural disasters.

**Develop policy to cultivate "reciprocity at scale."** Through the Cloud Safe Task Force collaborations, MITRE has heard from industry participants a desire to expand FedRAMP reciprocity. Because a FedRAMP Provisional Authorization (PA) is only used by the U.S. government, it has not been adopted by industry and is not necessarily useful for serving non-federal government consumers. Additionally, the FedRAMP Program Management Office (PMO) does not have reciprocity agreements regarding common industry certifications such as American Institute of Certified Public Accountants (AICPA) System and Organization Controls; CSA Security, Trust, Assurance and Risk; International Organization for Standardization (ISO); Payment Card Industry Data Security Standard; Cybersecurity Maturity Model Certification; and General Data Protection Agency. As a result, the cost for CSPs can be extreme when they are forced to acquire security certifications to serve specific consumers. This situation undermines a CSP's ability to deliver low-cost commodity IT services. FedRAMP policy could be revised to address compensating consideration for pre-existing industry certifications and to promote usage by industry bodies.

On page 6, consider encouraging more joint-agency authorizations.

Regarding Section III on page 4, while FedRAMP is intended to support an "authorize once, use many approach," this clause implies defining a separate authorization path for cloud systems used by a single agency. This could potentially cause agencies to re-authorize a new FedRAMP-

[6] NIST SP 800-160 Vol. 2 Rev. 1, Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. 2021. National Institute of Standards and Technology, https://csrc.nist.gov/pubs/sp/800/160/v2/r1/final. Last accessed December 12, 2023.

[7] MITRE CREF Navigator. 2023. MITRE, https://crefnavigator.mitre.org/navigator. Last accessed December 12, 2023.

[8] NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations. 2020. National Institute of Standards and Technology, https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final. Last accessed December 12, 2023.

hardened environment if it becomes a "cross-Government shared service," creating additional work and not fulfilling the intent of the FedRAMP Authorization Act.

In Section VII, Section d on page 15, points 2 and 3 could be challenging depending on the machine-readable and interoperable format chosen. Not every governance, risk, and compliance (GRC) tool supports certain formats chosen here, and implementing changes and/or replacing GRC tools may not be possible. While Open Security Controls Assessment Language (OSCAL) provides a solution, consideration should be given for use or interoperability with non-OSCAL compliant GRC tools.

On page 10, consider leveraging industry certifications like AICPA System and Organization Controls Report Type 2 and ISO27001[9] when establishing standards for accepting external cloud security frameworks and certifications. This may require NIST be tasked, rather than FedRAMP, to officially map existing FedRAMP/NIST controls to industry certifications that can then serve as an authoritative source for control mappings.

Regarding the concept of "multiple authorization structures" discussed on pages 3 and 6-7, it's important to note that the DoD usually can't use FedRAMP since it requires additional measures (with a DoD PA). FedRAMP might consider addressing this issue by providing a level of authorization that is acceptable to the DoD. Other USG organizations might welcome using more secure services as well. A DoD-wide authorization could prove more beneficial than multiple joint-agency authorizations. While this new policy opens the door to a DoD-wide authorization, it would help to provide clearer guidance on this matter as there is already an organization in the DoD, DISA, that provides DoD PAs for cloud services.

**Enhance oversight and governance.** Agencies should be required to submit Assessment and Authorization (A&A) artifacts to FedRAMP in a timely manner (i.e., within 30 days of agency issuance). All agency authorizations, regardless of type, should be presented in the FedRAMP Marketplace. This should include detailed information on status, evaluation results, intended actions and Plan of Action and Milestones. This information should be comprehensive enough for other agencies to understand, re-use the cloud service, and/or coordinate efforts for Authorizations to Operate (ATOs) currently planned or in process.

Agencies should also report significant incidents and the affected cloud services to the FedRAMP PMO with 48 hours of identification of the incident. Information about the nature and status of the incident will need to be sufficient for other agencies to evaluate the threat to their own environments and/or to coordinate responses.

The FedRAMP PMO is responsible for collecting, tracking, and disseminating significant evaluation and incident information to agencies and industry in a timely manner. Automation in the form of a central repository of information, available to agencies and industry, will enable sharing about the process of services through the ATO process, status or current ATOs, status of incidents, coordination efforts, and other pertinent information.

**Clarify authorization**. Apart from the specific duties of the FedRAMP Director, it is unclear who has the specific authorities to perform the roles and responsibilities of the multiple boards. Accountability is also not specified, nor is the understanding of the application of the shared

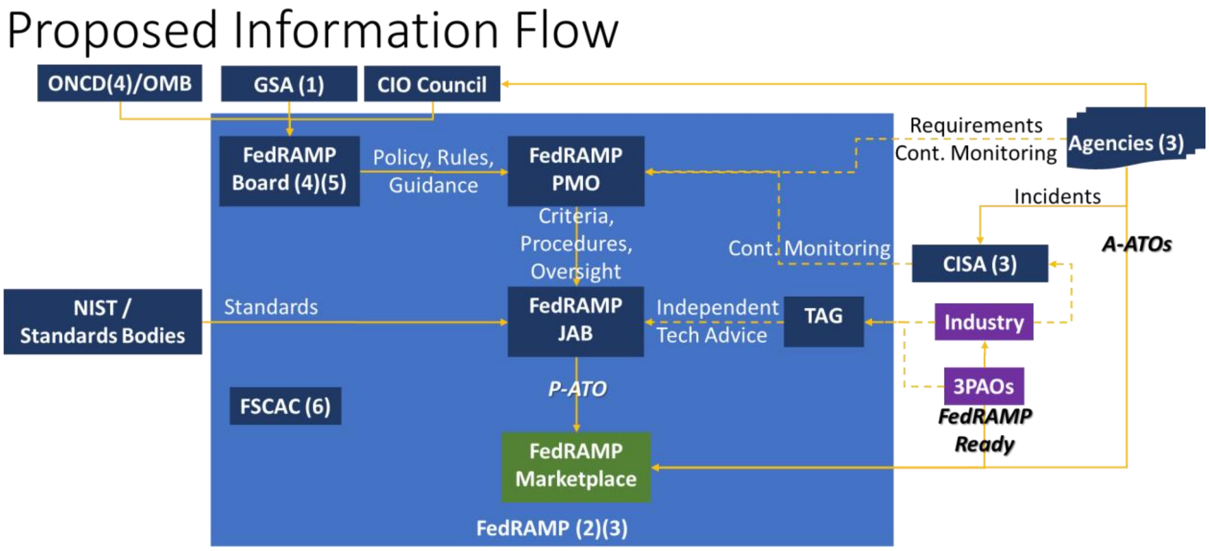
[9] ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection. 2022. International Organization for Standardization, https://www.iso.org/standard/27001. Last accessed December 12, 2023.

responsibility model to the oversight, management, maintenance and security monitoring, and operations of cloud services.

**<u>Define the shared responsibility model</u>**. The government must maintain responsibility for the security of its IT systems. Delegation of the implementation of security to cloud service providers is rational and preferred. This shared responsibility will vary between services and providers. A framework for documenting specific responsibilities should be included with the Provisional ATO (P-ATO) (for all types).

## FedRAMP Organization and Processes

Throughout the document, references are made to multiple boards and organizations internal and external to FedRAMP, and the roles and functions they perform. A detailed analysis of the roles, responsibilities, and functions of these organizations, and the information, direction, and influence that flows between them suggests the current proposal will result in bottlenecks, missing information for critical decision making, and overall poor results. If the intent is to streamline FedRAMP processes, then the right information must flow from organization to organization in such a way that it is available when needed. Further, no single organization should have so many responsibilities that it becomes a bottleneck to forward progress. The following diagram outlines a suggested improved information flow and distribution of responsibilities to streamline FedRAMP processes.



(1) Criteria for prioritizing products and services, prioritize for agency demand
(2) Establish standards for accepting ***external*** cloud security frameworks and certifications
(3) Shared monitoring between FedRAMP, CISA and Agencies
(4) Federal CIO & Office of the National Cyber Director must attend board meetings
(5) Requirements & Guidelines for Security Authorizations
(6) Missing connections between FSCAC and other boards and organizations related to FedRAMP

The memo references working with the CIO Council, but the role of the Federal CIO is not indicative of the support needed from the Federal CIO; "OMB-through the Federal CIO, will participate in board meetings." The memo also states that "the Director of ONCD may attend board meeting when appropriate" (top of page 14). The Federal CIO and the Director of ONCD should instead have clear leadership roles. GSA needs the support of the Federal CIO and ONCD as this is a matter of national defense.

The final section on industry engagement needs to clarify who the "front door" is for industry engagement. It is not clear if industry should go to GSA, the Board, or the PMO to engage. This was also a noted complaint by industry members participating in recent discovery sessions conducted by the MITRE Cloud Safe Task Force. This would be a great role for the Federal CIO and, probably more appropriately, ONCD.

For the FedRAMP model of "do once, use many times" to be optimized, agencies must fully support this model. While every agency of the U.S. government has a unique mission, the security of IT systems is most efficient and effective when standards and best practices make security management practical. To that end, ALL participating U.S. government agencies must accept the "presumption of adequacy" of FedRAMP P-ATOs, and understand the various types of ATOs outlined above and how to best leverage them, including the limitations, circumstances, operational security, shared responsibilities between government and the CSP, and any other factors.

## Additional Comments and Recommendations

**Establish a U.S. government-backed risk and vulnerability discovery program**, based on continuous vulnerability and penetration testing, to complement FedRAMP assessment and continuous monitoring activities. Today, Third-Party Assessment Organizations (3PAOs) are not empowered to perform routine, and potentially automated and AI/ML-enabled, penetration testing as part of assessments and continuous monitoring.

Aside from Bug Bounty programs implemented by the DoD and DHS, the U.S. government neither operates nor supports an active government-wide penetration testing program. Furthermore, there is little equivalent in industry where penetration testing skills and capabilities can be developed and maintained, and related vulnerabilities discovered for the common good. Ethical hacking practices, which aim to discover and inform without causing harm, could be implemented on a national level with proper regulation and FedRAMP oversight for cloud systems.

Determining how best to apply limited cybersecurity resources for maximum impact is a known challenge. Threat-based penetration testing is recognized as a viable approach to vulnerability discovery and is recommended by FedRAMP in guidance to the 3PAO assessment community. The MITRE Center for Threat Informed Defense[10] has demonstrated the development of Advanced Persistent Threat actor scenarios from elemental adversary Tactics, Techniques, and Procedures identified in the MITRE ATT&CK® Framework.[11] Further, the MITRE Caldera™ tool[12] and others can be applied for automated adversarial emulation. Pen-testers can use such

[10] MITRE Center for Threat Informed Defense. 2023. MITRE Engenuity, https://mitre-engenuity.org/cybersecurity/center-for-threat-informed-defense/. Last accessed December 12, 2023.

[11] ATT&CK®. 2023. MITRE, https://attack.mitre.org/. Last accessed December 12, 2023.

[12] Caldera. 2023. MITRE, https://caldera.mitre.org/. Last accessed December 19, 2023.

capabilities during the assessment process, and on a routine basis, to continuously test CSP and agency security posture. Automated and continuous testing programs can also be optimized to reduce costs and improve effectiveness with emerging AI/ML solutions.

Cost and liability considerations currently constrain the inclusion of penetration testing in FedRAMP continuous monitoring activities. To enable 3PAOs or specialized industry experts to conduct pen-testing for FedRAMP authorization and continuous monitoring, federal policy should be developed that mandates ethical practices and indemnifies CSPs from liabilities associated with potential service disruptions resulting from routing pen-testing activities. Additionally, every program for continuous testing against cloud systems must be developed and coordinated with the assistance of the CSP.

### Enhance the availability, visibility, and consumer utility of FedRAMP A&A packages and artifacts.

Currently, obtaining CRM and Controls Implementation Summary artifacts is challenging. Access is granted only to government personnel or their delegates and is terminated within 90 days. When available online through established Government-Cloud accounts, access must be specifically requested by privileged users and granted by CSP document owners. This slow and cumbersome process does not promote the open interchange of CSP control design and implementation details, leading to persistent gaps in knowledge regarding cloud service security. Furthermore, the necessary details to fully understand CSP security capabilities and the distinctions between "Common," "Hybrid," and "System" level controls are often not provided in the packages. FedRAMP should make CRM and Common Information Model (CIM) artifacts more comprehensive and readily available.

The materials gathered and produced by 3PAOs today are not made available to consumers nor shared with other assessors. One issue limiting reciprocity is the lack of a shared understanding of assessment practices. Different agencies and 3PAOs may assess control compliance in varying ways. Although technical assessment methodology and results can be sensitive, FedRAMP should establish an assessment community with the rights, privileges, and motivations to share assessment techniques and findings, facilitating a broader common understanding of evolving best practices for assessment.

One agency's A&A approach may not suit another's needs. In some cases, one agency may disagree with how another agency performs assessments. This potentiality can limit the adoption of reciprocity practices, which are central to the FedRAMP mission. Additionally, variations in risk appetites or risk aversion/acceptability across agencies can affect reciprocity. This issue can be addressed, in part, by including "Threat-Risk Profiles" as part of a CSP's A&A package. An agency is more likely to accept another agency's ATO if it feels confident that the ATO addresses its threat-risk profile. Specifying the threat surface addressed by an A&A activity facilitates better communication and a common understanding of the value of the A&A activity and the associated ATO.

A long-standing issue for cybersecurity practitioners in the cloud is related to CSP practices surrounding the introduction and documentation of new services and the apparent FedRAMP PMO acceptance of the practice. Often, when CSPs add new services to a previously authorized FedRAMP environment, they do not provide a CRM or similar guidance for the new services. Consequently, consumers are routinely left to figure out how to design and implement necessary hybrid and system controls to secure the use of the service and achieve compliance. In some cases, costly consulting engagements with the CSP or outside experts may be required. FedRAMP guidance and requirements for CSPs to adhere to in this regard would promote new service adoption and reduce the costs of security implementation.

**Streamline processes through automation and integrating FedRAMP into pre-production operations.**

On page 4, the point about "Leverage shared infrastructure" addresses the feature mismatch between "Commercial Cloud vs GovCloud." A common issue is that services and capabilities are rolled out to the commercial side and only made "FedRAMPed" or released for GovCloud months or years later. Rapidly building a new service with extensive functionality but without meeting core security needs has been a major inhibitor to agility and speed. The "first to market" rush mentality often leads to "adding security later," a prevalent problem at the intersection of innovation and security. FedRAMP must integrate with innovators to facilitate the adoption of security solutions early in the product development lifecycle.

OMB should develop a comprehensive IT compliance framework to consolidate and align IT compliance processes, including FedRAMP, Security Authorization, Authority to Operate, System of Records Notices, Privacy Impact Assessments, and Paperwork Reduction Act requirements. This framework should outline all IT compliance requirements and standards, be based on OMB requirements and NIST guidelines, and be updated continuously to reflect changes in technology, threats, and regulations.

At present, vendors report that the FedRAMP certification process takes 18–24 months, as do Security Authorization and ATO approvals and final System of Records Notice (SORN) approvals. A new compliance framework should streamline approvals and allow systems and projects to ramp up more quickly. Accelerated approvals will allow both the government and private sector to keep pace with artificial intelligence developers worldwide who do not face 18–24-month compliance requirements for setting up AI systems.

Both cloud providers and consumers are working to automate security functions and build secure systems using Infrastructure-as-Code (IaC). Today, the IaC-based DevSecOps pipeline is the modern software supply chain. As such, many security vulnerabilities can be mitigated in a pre-deployment segment of the pipeline, but the pipeline can also serve as an entry point for malware injection. Consequently, the DevSecOps pipeline provides an opportunity for FedRAMP to leverage inherent automation capabilities in cyber assessment and integrate assessment operations into pre-deployment segments of the CSP's software supply chain. NIST's development of OSCAL standards and FedRAMP's acceptance of A&A artifacts in OSCAL form are steps in the right direction but do not fully integrate FedRAMP PMO into pre-deployment system assessments. 3PAOs should be allowed to assess the adequacy, hardening ability, and resiliency of CSP DevSecOps pipelines. By becoming an integral part of CSP IaC-based DevSecOps pipelines, the FedRAMP PMO will be better positioned to leverage the inherent cloud-native automation capabilities and more agilely perform A&A activities. This would necessitate a revamping of FedRAMP PA processes to require early integration of FedRAMP A&A processes and data sharing connections.

The DoD's Iron Bank provides an example of a secure code repository that could be applied at the federal level. Each container in the federal repository would include: 1) a Software Bill of

Materials (SBOM) and 2) assessment evidence for the container (e.g., results of Static Application Security Testing and Dynamic Application Security Testing) for Authorizing Officials (AOs) to make their own risk determination. Government agencies and organizations could vote on containers to evaluate, and FedRAMP would select which ones to evaluate, partly based on those votes. Containers that pass scrutiny would become available in the federal repository. Like Iron Bank, containers would include both commercial and open-source software. Ideally, if a vulnerability is found in some component (e.g., Log4J), a tool could scan the SBOMs in the repository and notify those who have downloaded the containers about the issue. While this extends beyond cloud services, it is a crucial component in supply chain risk management for dominating the cloud security operational space. Moreover, many of the services FedRAMP evaluates are essentially a set of containers or virtual machines (VMs) running on one of the major commercial clouds (AWS, Azure, etc.).

On page 9, the memorandum requires GSA and the FedRAMP program to establish an automated FedRAMP security assessment and review capability by December 23, 2023. Considering the breadth and scope of the task, this deadline should be extended to within 90 days of the memorandum's issuance.

**Address the need for AI/ML enabled cross-CSP threat detection and response capabilities** derived from FedRAMP's continuous monitoring data sources.

Currently, FedRAMP receives monthly vulnerability scan reports from authorized CSPs. This reporting frequency is insufficient to respond to today's cyber-attacks. Additionally, information from these reports is not cross-correlated so that one CSP's vulnerability discovery can be used to drive discovery and remediation for other CSPs. This is a role FedRAMP can play, given that vital data is already being captured. As continuous monitoring reports are received, the FedRAMP PMO should apply AI/ML capabilities to detect cross-CSP vulnerabilities and provide warning indicators to CSP management and cloud consumers. Associated information can give the cyber defender a head start on implementing threat mitigations.

Enhancing the frequency of reporting and incorporating a Cloud Bill of Materials (BOM) that covers hardware, software, and firmware will enhance the detection of vulnerabilities in cloud services and support the correlation of vulnerabilities across different CSPs. The FedRAMP continuous monitoring policy could be updated to mandate these data feeds with increased regularity, thereby constructing a database for cross-BOM correlation analysis. This would empower the FedRAMP Program Management Office (PMO) to play a more immediate and significant role in cloud defense.

**Address shared responsibility and the "presumption of adequacy."**

A significant and evolving issue not covered here is the CRM. CSPs are granted FedRAMP approval by documenting and demonstrating that they meet all the controls and requirements EXCEPT for those listed as a customer responsibility. In the past, it was believed that only CRM items that apply to Defense Acquisition Regulation Supplement/NIST SP 800-171 needed to be implemented by customers to ensure a FedRAMP environment and meet NIST 800-171 compliance. However, recent guidance suggests that unless customers meet ALL controls listed in the CRM (even those that are NIST SP 800-53 and not NIST SP 800-171), the environment does not actually meet FedRAMP requirements, which for some CSPs adds a considerable additional burden of security/compliance controls. Clarity about CSPs "meeting" FedRAMP by offloading requirements to customers and what that means for actual implementation would be beneficial.

On page 5, Section IV, paragraph 1 ("agencies must presume that assessment documented in the authorization package is adequate for their use in issuing an authorization to operate"): Currently, all FedRAMP packages include agency-specific controls that need to be implemented and an ATO decision by the agency AO. The current wording implies that agencies have no additional responsibilities when leveraging a FedRAMP authorization and that those controls do not require additional validation when implemented. Unless this signifies a change in the FedRAMP program, this statement may need revision.

**Enhance national security leadership and technical advisory.**

The requirement on page 15 for the Technical Advisory Group (TAG) to consist of six technical experts seems like a small number, especially with cloud technologies advancing so rapidly that SMEs are now specializing in a specific CSP. We have also heard from industry peers concerned that federal employees may not have sufficient technical depth to succeed on this matter alone. One way to add technical depth while maintaining a government-centric focus, and without introducing bias, would be to leverage SMEs from FFRDCs on the TAG in some capacity.

Regarding references to the Board establishing a technical working group for CSP review (see continuous monitoring section, bottom of page 11), it is reasoned that the implied activity should be a function of the TAG.

**Enhance continuous monitoring.**

Section VI: In line with OMB Circular A-130[13] and NIST SP 800-137, agencies are required to adopt and implement privacy continuous monitoring (PCM) programs. PCM aids in identifying potential privacy risks and vulnerabilities in real time, enabling agencies to address them before they escalate into more significant issues.

Section VI: Incorporating PCM requirements into the FedRAMP process will not only ensure compliance with OMB and NIST requirements, but also safeguard personal information, thereby demonstrating the government's commitment to privacy. PCM helps to identify and address privacy risks proactively, adapt to evolving threats, and maintain the public's trust. The FedRAMP update should include PCM requirements.

**Support innovation and competition by small and medium-sized businesses.**

Small and medium businesses represent at least half of technological innovations that act to continuously improve government functions and missions. They simply cannot survive the cost and schedule involved in obtaining FedRAMP certifications. Some have actually failed waiting for FedRAMP to act. U.S. government small business programs could be designed to incentivize new small and medium sized businesses to participate in the FedRAMP program through financial support and fast-tracking the auditing and accreditation processes, providing education and information about the FedRAMP processes, and dedicating 3PAOs to specialize in new small and medium business evaluations.

[13] Circular A-130, Managing Information as a Strategic Resource. 2016. Office of Management and Budget, https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf.

**Address Multi-Cloud.**

Multi-Cloud integration increases integration and governance complexity and may open an adopting organization to unexpected threats. Individual CSPs receive FedRAMP authorizations for specific services. Yet the government may need to integrate multiple services from multiple CSPs to support missions. FedRAMP should consider working with NIST to provide Multi-Cloud security control guidance, for Inter-Cloud security integration and management. A schema for Inter-Cloud Inheritance in assessment and authorization may also help speed agency authorizations. CSPs and 3PAOs could be asked to include documentation in their submission packages that describe the integration concepts associated with their service offerings. This would provide agencies with initial guidance on implementing security in a Multi-Cloud environment, including Application Program Interfaces, automation, logging, interoperability, and governance in a Multi-Cloud environment. The FedRAMP PMO should consider collaborating with DHS's Cybersecurity & Infrastructure Security Agency to develop Multi-Cloud Security Implementation Guidance.

**Suggested areas for greater document detail or revision:**

- Page 2: What does "expert program" mean? Remove the word "expert" or provide detail.
- Page 3, Vision, third paragraph: Focused on changes in needs of federal agencies but doesn't address the changes in the cloud marketplace or in cyber threats and the capabilities to address those threats in the past 12 years.
- Page 4, "FedRAMP should not incentivize or require commercial cloud providers to create separate, dedicated infrastructure for Federal use": While this is an ideal scenario, the challenge of hosting Impact Level (IL) 5 (or higher) services and data on an IL 2 commercial cloud has not yet been resolved. For instance, there's the requirement for data center employees to be 'US Persons' for IL5. Similarly, on page 11, the statement 'Avoids incentivizing the bifurcation of cloud services into commercially-focused and Government-focused instances' is mentioned. If DoD requirements cannot be met, it may be advisable to reconsider these statements.
- Page 4, Section III, paragraph 2: "Host information systems" is problematic here as Software as a Service (SaaS) services often process/store/transmit government data but wouldn't be considered a "host." Often, SaaS solutions are leveraged as part of a larger Federal Information Security Management Act (FISMA) Information System but may not be considered a host (like Infrastructure as a Service). In the examples that follow, federal information is used as a delineating term and should be considered as the term used here.
- Page 5, Section IV, first paragraph: The last sentence seems to say any level of FedRAMP authorization is adequate for any ATO. That doesn't seem right for ATOs that require higher-level security. The following paragraph addresses this but then minimizes it in the last sentence at the top of page 6.
- Page 6, first full paragraph: Recommend removing "For this presumption to be useful,"
- Page 6, Section IV, item 1: Is the single-agency authorization required to use the FedRAMP authorization process (similar to current processes) or does this imply that the AO can authorize a cloud system using the agency's authorization process (and risk tolerance)?

- Page 6 & 7: It would be beneficial to have the documentation behind the authorization available to other agencies so that they can make a decision on whether the authorization is adequate.
- Page 7, number 3: It would be beneficial to have the documentation behind the ATO to be available for agency review.
- Page 7, Section IV, item 2: Does the joint-agency authorization result in a P-ATO or does this still go through the FedRAMP PMO review once multiple agencies authorize a system? Are the agencies required to use the FedRAMP authorization process with FedRAMP PMO reviews or can they define their own process?
- Page 7, Section IV, item 3: Is this replacing or the same as the current Joint Authorization Board authorization?
- Page 9, Section IV, final paragraph: It would be helpful to know if it's 12 months from the pilot to get FedRAMP authorized or to start the FedRAMP authorization process (which has traditionally taken 9–12 months).
- Page 10: This seems to be trying to discuss (or SHOULD be discussing) leveraging DevSecOps for development of new FedRAMP services/capabilities—vetting the security as integrated into the development of cloud services would help accelerate the testing/adoption of new FedRAMP services. It's covered later but seems like it should be called out here.
- Page 11, Section VI, paragraph 2, bullet 2: No minimum time is defined for advanced notice.
- Page 11, Section VI, paragraph 3: "When finalized..."—What is the role for agencies at this point? How do agencies understand risk posture?
- Page 11: Consider defining with greater detail the monitoring standard described in the second to last paragraph.
- Page 12, Section VI, paragraph 6: Does the FedRAMP PMO hold the authority to revoke an authorization based on continuous monitoring performance? If so, how do agencies respond?
- Page 17: The memorandum requires each agency to create or update a policy within 180 days of issuance of the final memorandum that promotes the use of secure cloud services as determined by OMB, GSA, and CISA. Worth adding that each agency should ensure it allocates sufficient resources to meet this deadline.
- Page 17: The memorandum also requires the FedRAMP program to update its continuous monitoring processes and documentation within 180 days of issuance of the memorandum. Furthermore, GSA has 18 months from the issuance of the memorandum to implement a fully automated, machine-readable capability for receiving FedRAMP authorization and continuous monitoring artifacts. Worth calling out that this aggressive timetable will require GSA and its FedRAMP partners to allocate sufficient resources for this collaborative effort.

- Page 17: The memorandum calls for FedRAMP to develop a plan to help agencies move off cloud infrastructure designed solely for government use within a year. This plan should encourage agencies and commercial providers to integrate security practices into their core services that rely on a zero trust approach to cloud security. As such, the memorandum should also reference the initiatives detailed in OMB M-22-09.