# MITRE's Response to the FedRAMP RFI on Metrics

## August 29, 2024

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 organization dedicated to advancing the public interest by addressing some of the nation's most challenging issues related to safety, stability, security, and overall well-being. We manage several Federally Funded Research and Development Centers (FFRDCs), engage in Public-Private Partnerships across national security and civilian sectors, and drive independent technology research in key areas like artificial intelligence, data science, quantum information, health informatics, policy and economic analysis, trustworthy autonomy, and cyber resilience.

With a workforce of approximately 10,000 professionals, MITRE is committed to solving complex problems through a multidisciplinary approach, upholding scientific integrity as the cornerstone of our work. Unlike other organizations, we do not engage in lobbying, product development, or sales. We have no owners or shareholders and do not compete with industry, ensuring that our work is objective, data-driven, and free from political or commercial bias.

MITRE has a proven track record of supporting federal agencies in securely adopting cloud technologies to enhance mission outcomes. Our expertise includes navigating certification processes such as the Federal Risk Authorization Management Program (FedRAMP) and developing the Enterprise Cloud Adoption Framework (ECAF). Recognized by the General Services Administration as a best practice, the ECAF is a comprehensive tool that assists leaders in navigating all aspects of cloud adoption, from policy to technology, and has gained international acclaim.

MITRE established the Cloud Safe Task Force (CSTF) in response to recent cyber breaches targeting government IT infrastructure—many attributed to state actors. Collaborating with federal government, industry, and not-for-profit partners, including the Cloud Security Alliance (CSA), the CSTF addresses critical gaps in cyber resilience, particularly in certification processes and known vulnerabilities. The task force aims to strengthen the security of vital digital infrastructure. Through a series of meetings and published recommendations, the CSTF has provided a roadmap for securing government cloud services and improving continuous monitoring via cloud service providers' (CSPs') dashboards. These recommendations, combined with MITRE's own insights, form the foundation of our approach to bolstering the security of the nation's digital assets.

# Overarching Recommendations

MITRE recommends that FedRAMP expand its metrics approach to enhance its effectiveness beyond the traditional scope of the cost and timeliness of the program. This rethink is needed to address rising costs, improve security performance, and foster innovation by reducing redundant assessments and streamlining compliance. By adopting more meaningful and real-time metrics, FedRAMP can better ensure the security of cloud services, enhance national cybersecurity, and facilitate faster deployment of secure cloud solutions.

MITRE's extensive experience with the cloud services community, gained through assisting government agencies in defining adoption strategies, planning and implementing migration programs, and addressing security implications to deliver robust cloud-based security

governance and operations, provides it with a unique perspective. More recently, MITRE has been actively involved in the Department of Homeland Security Cybersecurity and Infrastructure Agency's Secure Cloud Business Applications cloud hardening programs. In this RFI response, MITRE presents concepts to enhance FedRAMP's effectiveness. This response provides specific recommendations addressing:

- Rethinking FedRAMP Processes and Metrics to Drive Reciprocity
- Measuring Reciprocity as an Indicator of Industry Cost of Authorization
- Rethinking FedRAMP Measures of Effectiveness to Drive Improvements in Operational Cyber Performance and National Security
- Rethinking FedRAMP Continuous Monitoring Metrics to Improve National Security
- Rethinking FedRAMP Continuous Monitoring with Continuous Testing.
- Rethinking FedRAMP Metrics to Support Adoption of Quantum Resistant Cryptography and Zero Trust Initiatives

## Rethinking FedRAMP Processes and Metrics to Drive Reciprocity

The assessment and authorization (A&A) process, which is rooted in the Federal Information Security Management Act (FISMA) policy, the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF), and FedRAMP requirements, plays a critical role in cyber governance. However, the rising costs associated with these processes are now limiting innovation, competition, and the timely refresh of services available to the government. Considering the multiple A&A frameworks that today's CSPs must navigate for national and international compliance, MITRE introduces the concept of Reciprocity-at-Scale (RaS).

RaS acknowledges that an individual cloud service's security controls are often assessed multiple times to comply with multiple different A&A frameworks. Rather than reducing the rigor of these assessments, RaS advocates for the effective reuse of assessment information across agency RMF activities, national A&A frameworks (including FedRAMP), and international A&A frameworks. Under RaS, if a cloud service has already undergone a security control assessment, and the controls are deemed equivalent to ones assessed under another agency's RMF or A&A framework, the CSP should not need to undergo a redundant reassessment of the same controls or inter-related sets of controls. The benefits to government and industry providers of MITRE's proposal to re-evaluate FedRAMP A&A metrics and implement RaS include:

- **Benefit to Government**: Implementing RaS allows the government to recognize certifications and authorizations across different frameworks and jurisdictions, reducing duplication of effort and accelerating the deployment of secure cloud services. This approach can also facilitate international collaboration and alignment in cybersecurity practices.
- **Benefit to Industry Providers**: RaS reduces the need for CSPs to undergo multiple, often redundant, A&A processes for different regulatory frameworks. This not only lowers compliance costs but also simplifies the process of expanding services into new markets, both domestic and international.

Implementing RaS will be complex and will require time. Several factors contribute to these complexities, including:

- Differences in security control structures, content, and context across A&A frameworks
- Inconsistencies in assessment techniques among different assessors and frameworks
- Differences in authorities and approval processes across agencies
- Discrepancies in IT system designs and their security control implementations
- Disparities in threat surfaces across IT systems
- Variations in risk profiles among IT system owners and stakeholders

To support reciprocity negotiations and move toward RaS, standardization is essential to create universal acceptance and reciprocity in the following areas:

- Security control standards
- Control assessment techniques
- A&A processes
- Control assessment reporting methods and artifacts

While some standards already exist, many require updating to reflect advancements in methods, processes, reporting, and the ever-evolving cloud landscape. For example, NIST SP 800-115, a guide for information security testing and assessment, was last updated in 2008, early in the evolution of cloud technology. Similarly, while recent updates have been made to NIST RMF documents, significant differences remain between U.S. and European Union (EU) A&A frameworks. The European Network and Information Security Agency (ENISA) released its Cloud Computing Information Assurance Framework in 2009. There is potential for national standards updates and international collaboration on standards, creating opportunities for joint cyber security protections that would improve national security in the United States and the EU. ENISA is currently leading an effort to standardize security compliance across Europe through proposed European Union Cybersecurity Scheme (EUCS) legislation. The CSA, an international[1] organization, has been working with NIST, ENISA, and other bodies to evolve cloud security standards and practices. Because U.S. CSPs tend to operate internationally, MITRE proposes leveraging current CSA and ENISA efforts to grow alliances between the United States and EU that promote RaS cooperation.

MITRE has also developed several frameworks that might be adapted for use in communicating the efficacy of security capabilities, thereby promoting RaS:

- ATT&CK® for threat-driven assessment[2]
- D3FEND™ for security capability implementation assessment[3]

[1] EUCS- Cloud Services Scheme. 2024. European Union Agency for Cybersecurity, https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme. Last accessed: August 27, 2024.

[2] ATT&CK. 2024. MITRE, https://attack.mitre.org/. Last accessed: August 22, 2024.

[3] D3FEND. 2023. MITRE, https://d3fend.mitre.org/. Last accessed: August 22, 2024.

- Government Cybersecurity Architecture Review (GovCAR) for gap analysis[4]
- Adaptive Capability Assessment (ACT) for both manual and automated assessment[5]
- Security Automation Framework® (SAF) for automated compliance hardening and testing

These frameworks, and others like them, could be leveraged by cybersecurity engineers to modernize security and compliance testing. By harmonizing standards, we can enhance the ability of stakeholders to negotiate effective reciprocity agreements, ultimately leading to a more secure and efficient cloud service environment for the government.

The CSTF has recommended shifting from a compliance-based evaluation of security to an approach that measures real-world effectiveness. This approach will yield better results in protecting national assets and fostering mutual trust between federal government and industry partners within the cloud's shared responsibility model. Therefore, MITRE proposes a re-evaluation of the metrics used in the FedRAMP A&A processes to better address cybersecurity effectiveness and the value of reciprocity.

The significant costs imposed on industry due to these processes directly affect the cloud services available to the government, underscoring the need for this rethinking. The burden placed on the government to manage this ever-growing program would also benefit from new approaches. The following table provides a list of suggested metrics FedRAMP might employ to measure and foster reciprocity within the industry.

| Metric and Description | Objective | Benefit to Government | Benefit to Industry |
|---|---|---|---|
| ***Framework Commonality Assessment:*** Evaluates the similarities and differences between the FedRAMP authorization process and controls with those of other U.S. and international security frameworks. It measures the degree of commonality between these frameworks. | To understand how closely aligned FedRAMP is with other security frameworks, facilitating the identification of opportunities to streamline the authorization of new services across multiple frameworks by leveraging shared controls and assessments. | Allows government agencies to more efficiently assess and approve cloud services that meet multiple security standards, reducing duplication of effort and speeding up the authorization process for services that adhere to common frameworks. | For CSPs, this assessment highlights the potential to reduce the cost and complexity of achieving compliance with multiple security frameworks, enabling them to offer services that meet diverse regulatory requirements with minimal additional effort. |

[4] CDM Program. What Is .govCAR?. 2020. Department of Homeland Security/Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/sites/default/files/publications/2020%2009%2003_%20CDM%20Program%20govCAR_Fact%20Sheet_2.pdf.

[5] MITRE Adaptive Capabilities Testing (ACT) for Risk-Based Decision Making. 2023. MITRE, https://www.mitre.org/sites/default/files/2024-02/PR-23-3222-MITRE-Adaptive-Capabilities-Testing-Risk-Based-Decision-Making.pdf.

| Metric and Description | Objective | Benefit to Government | Benefit to Industry |
|---|---|---|---|
| ***Framework Reciprocity Score:*** Measures the number of cloud consumers and government agencies that are leveraging each specific security framework, providing an indication of the framework's adoption rate or "market share" within the federal government. | To assess the popularity and active usage of different security frameworks within the federal government, providing insights into which frameworks are most trusted and widely used. | Enables government agencies to identify and prioritize frameworks that are widely adopted and trusted across the federal landscape, ensuring alignment with prevailing security practices and potentially improving interoperability among agencies. | For providers, understanding the adoption rate of specific frameworks helps in making strategic decisions about which frameworks to pursue, ensuring that their services meet the most widely recognized and valued standards in the market, thereby enhancing their competitiveness. |
| ***Service Reciprocity Score:*** Tracks the number of authorizations and the list of frameworks, both U.S. and international, under which a cloud service has been certified. It provides a comprehensive view of a service's authorization status across various security standards. | To provide transparency regarding the compliance and certification status of cloud services across multiple security frameworks, facilitating informed decision making by both government agencies and service providers. | Offers government agencies a clear understanding of the security credentials of cloud services, allowing them to select services that meet their specific security requirements and are recognized across multiple frameworks, enhancing trust and reducing risk. | For CSPs, a high Service Reciprocity Score indicates broad acceptance and certification across various frameworks, boosting marketability and customer confidence. It also simplifies the process of demonstrating compliance with multiple security standards, making it easier to enter and expand in different markets. |
| ***Percentage of CSPs Leveraging Existing Authorizations:*** Measures the proportion of CSPs that reuse existing FedRAMP authorizations from one federal agency to gain authorization with another, rather than undergoing separate authorizations. | To measure how effectively CSPs utilize the reciprocity principle to streamline their certification process across multiple federal agencies. | Reduces redundancy and the need for multiple agencies to conduct the same security assessments, saving time and resources. | Lowers the cost and time required to gain authorization across multiple agencies, accelerating time to market for CSP services. |
| ***Cross-Agency Authorization Adoption Rate:*** Measures the rate at which FedRAMP-authorized CSPs are adopted by multiple federal agencies | To gauge the level of trust and recognition among federal agencies in accepting existing FedRAMP authorizations. | Promotes greater interagency collaboration and efficiency in adopting cloud services, leading to more uniform security | Encourages broader adoption of services across federal agencies, increasing market penetration and reducing the need for multiple assessments. |

| Metric and Description | Objective | Benefit to Government | Benefit to Industry |
|---|---|---|---|
| without requiring additional assessments or certifications. | | standards across agencies. | |
| ***Time to Reciprocity:*** Measures the average time it takes for a CSP's FedRAMP authorization to be accepted by additional federal agencies after the initial authorization is granted. | To assess the speed and efficiency of the reciprocity process, ensuring CSPs can quickly expand their services to multiple agencies. | Enables faster deployment of secure cloud services across agencies, reducing delays in service adoption and improving overall efficiency. | Reduces the lag between initial authorization and expanded adoption, enabling quicker service delivery to a broader range of government customers. |
| ***Industry Adoption of FedRAMP Authorized Services:*** Measures the percentage of private-sector companies that adopt cloud services from FedRAMP-authorized CSPs, demonstrating trust in the FedRAMP process. | To evaluate the recognition and adoption of FedRAMP standards by the private sector, indicating the broader market's trust in the program. | Validates the rigor and reliability of FedRAMP standards, reinforcing the government's security posture and potentially influencing private-sector best practices. | Enhances the reputation and credibility of FedRAMP-authorized CSPs, driving adoption in both the public and private sectors. |
| ***Reciprocity Utilization Ratio:*** Measures the ratio of FedRAMP-authorized CSPs utilized by more than one federal agency compared with those used by only one agency. | To assess the extent to which federal agencies are reusing FedRAMP authorizations, reflecting the program's success in fostering interoperability and trust. | Promotes more efficient use of government resources by encouraging agencies to leverage existing authorizations, reducing duplication of efforts. | Increases the likelihood of services being adopted by multiple agencies, enhancing market opportunities and reducing the need for repeated assessments. |
| ***Reciprocity Rejection Rate(s):*** Measures the percentage of instances where a CSP's existing FedRAMP authorization is not accepted by another federal agency, requiring additional reviews or assessments. | To identify barriers or challenges to reciprocity and pinpoint areas where the process can be improved. | Highlights areas where the FedRAMP process might be inefficient or inconsistent, providing data to improve the program and ensure smoother operations. | Reduces the risk of unexpected additional costs and delays, allowing CSPs to plan and execute their federal engagements more predictably. |

## Measuring Reciprocity as an Indicator of Industry Cost of Authorization

One of the key issues identified by the CSTF is the burden placed on CSPs that must undergo assessments and apply for certifications across multiple security frameworks, many of which lack reciprocity. This challenge is particularly acute for CSPs operating in various sectors, each

with its own set of security A&A requirements. For example, CSPs must navigate certifications for:

- Health care (Health Insurance Portability and Accountability Act, Health Information Technology for Economic and Clinical Health Act)
- Defense Industrial Base (Department of Defense Security Requirements Guide, Cybersecurity Maturity Model Certification)
- Automotive industry standards (Trusted Information Security Assessment Exchange)
- Payment card security (Payment Card Industry Data Security Standard)
- Quality management (International Organization for Standardization 9001)
- Finance and accounting (American Institute of Certified Public Accountants' Service Organization Control)
- Education (Family Educational Rights and Privacy Act)
- Tax preparation (Internal Revenue Service 1075)
- Cryptography (NIST Federal Information Processing Standard)
- Export regulations (International Traffic in Arms Regulations)

Furthermore, CSPs must also comply with numerous privacy and information security requirements to conduct business internationally, such as General Data Protection Regulation (European Union), Information Security Registered Assessors Program (Australia), Multi-Tier Cloud Security Tier 3 (Singapore), Korea Information Security Management System (Korea), Cloud Computing Compliance Controls Catalogue (Germany), and Esquema Nacional de Seguridad High (Spain).

This multiplicity of certifications often forces CSPs to reassess the same security controls multiple times, driving up costs and potentially delaying the delivery of cloud service offerings (CSOs). To address this issue, FedRAMP could begin by measuring the extent to which CSPs are required to reassess security controls to obtain FedRAMP Provisional Authorization. Such metrics could reveal the levels of duplication within the A&A industry, specifically related to FedRAMP control baselines.

Additionally, CSPs could report on the number of times a FedRAMP security control was assessed before the FedRAMP third-party assessment organization (3PAO) assessment, along with the frameworks in which these controls were previously evaluated. This data could be instrumental in discussions aimed at achieving greater reciprocity across different frameworks, thereby reducing redundant assessments. The anticipated cost savings from such cross-framework reciprocity could lead to increased innovation and faster updates to CSOs, ultimately benefiting both CSPs and their customers. The following table provides a list of metrics FedRAMP might employ to measure the cost of authorization.

| Metric and Description | Objective | Benefit to Government | Benefit to Industry |
|---|---|---|---|
| ***Authorization Fatigue Index (AFI):*** Measures the level of "authorization fatigue" experienced by stakeholders (CSPs) during the FedRAMP process. | To use surveys and other feedback mechanisms to assess factors like perceived bureaucratic burden, repetitive tasks, communication inefficiencies, and decision-making bottlenecks. The AFI would be a composite score indicating how taxing the process feels to participants. | A high AFI score might indicate areas where the process could be streamlined, or where additional support might be needed to keep stakeholders engaged and motivated. | Will better inform FedRAMP on areas for process improvement. |
| ***Adaptive Authorization Readiness Score (AARS):*** Develops a dynamic, real-time scoring system that evaluates a CSP's readiness for FedRAMP authorization based on its existing security posture, documentation quality, and prior compliance history. | Before starting the FedRAMP process, CSPs would complete a comprehensive self-assessment using a FedRAMP-provided tool. The AARS would score them on various criteria, providing a readiness score that predicts how smoothly their authorization process might go. | This score would help FedRAMP understand CSPs' preparation for assessment and their ability to reuse A&A artifacts. | This score would help CSPs identify gaps early, allowing them to focus on areas that need improvement before formally entering the FedRAMP process, thus reducing time and costs. |
| ***Cost Savings from Reciprocity:*** Measures the estimated cost savings achieved by federal agencies and CSPs due to the reuse of existing FedRAMP and other industry authorizations. | To quantify the financial benefits of reciprocity in the FedRAMP program, highlighting its value in reducing redundant assessments. | Demonstrates fiscal responsibility and the effectiveness of the FedRAMP program in conserving taxpayer dollars by avoiding unnecessary duplication of security assessments. | Provides a clear financial incentive for pursuing FedRAMP authorization, as it underscores the cost savings associated with reciprocity and broader federal market access. |
| ***Control Reassessment Frequency:*** Provides a score that indicates the relative number of times a FedRAMP security control was assessed before a FedRAMP assessment. | To quantify the degree to which a group of or individual security controls have been previously assessed for non-FedRAMP security certifications. | This score will help FedRAMP better understand CSP costs of assessment activities and the degree to which other certification frameworks are requiring the same controls. | This score could be used by CSPs to build a case for reuse of existing control assessment artifacts to avoid reassessment of the FedRAMP-required security control. |

## Rethinking FedRAMP Measures of Effectiveness to Drive Improvements in Operational Cyber Performance and National Security

While the current metrics related to the performance of A&A activities by providers, assessors, and authorizers are undeniably important, there is an increasing need for more meaningful measures that focus on actual security performance. The central questions that FedRAMP should be addressing—but currently is not—are:

- Does achieving FedRAMP compliance genuinely enhance the security performance of CSPs and their CSOs?
- Is FedRAMP operating to effectively deliver secure CSOs for government use?

The CSTF has advised the federal government to refine its performance metrics by transitioning to continuous monitoring that incorporates real-time and resilience-based cyber performance metrics.[6] The table below provides a comprehensive set of metrics designed to assess operational cyber performance, focusing on both effectiveness and resilience. These proposed metrics aim to provide a clearer understanding of how well FedRAMP is achieving its goals and ensuring that government agencies have access to secure and resilient cloud services. Additionally, reciprocity of A&A (or similar) approvals is expected to reduce time and cost for industry participation, leading to greater availability and use of innovative services.

To monitor progress in creating a more secure and resilient environment and provide meaningful insights to FedRAMP stakeholders, MITRE recommends use of a combination of technical and operational metrics that directly measure the effectiveness of security controls, the organization's overall security posture, and the cyber resiliency of CSOs.

Included with each potential metric is a brief explanation of how the particular security performance metric maps back to improving the FedRAMP experience for both customers and providers. This explanation involves demonstrating how these metrics enhance trust, transparency, and security effectiveness, which are core to the FedRAMP framework.

The proposed metrics focus on measuring the actual security posture and operational effectiveness of an organization rather than simply tracking compliance with regulations. By monitoring these metrics and sharing them with FedRAMP stakeholders, FedRAMP can demonstrate the government's commitment to maintaining a secure environment for its users and the vendor community can further demonstrate its commitment to continuously improving its security offerings.

[6] Cloud Safe Task Force: National Cloud Cyber Feed Initiative. 2024. MITRE, https://www.mitre.org/news-insights/publication/national-cloud-cyber-feed-initiative. Last accessed August 22, 2024.

| Proposed Metric | Description | Why It Matters | How This Improves the Experience for Customers and/or Providers |
|---|---|---|---|
| ***Mean Time to Detect (MTTD)*** | Measures the average time taken to identify a security incident from the moment it occurs. | A shorter MTTD indicates that the organization is effectively monitoring its environment and can quickly identify potential threats, which is crucial for minimizing damage. | By reducing the time it takes to detect security incidents, providers can quickly address threats before they escalate, thereby ensuring that FedRAMP-authorized systems remain secure. Customers benefit from knowing that their data is being protected by a proactive monitoring and detection approach, reducing potential downtime and data breaches. |
| ***Mean Time to Respond*** | Measures the average time taken to respond to and mitigate a detected security incident. | Reflects the organization's ability to contain and resolve security incidents, reducing the impact on the system and data. | Faster incident response times demonstrate a provider's capability to swiftly mitigate security threats, which aligns with FedRAMP's requirement for prompt incident handling. This builds confidence among customers that their service provider is equipped to handle security issues efficiently, minimizing impact on their operations. |
| ***Mean Time to Recover (MTTRc)*** | Measures the average time required to restore a system or service to full operational status after a disruption or failure. It is calculated by taking the total recovery time for all incidents within a given period and dividing it by the number of incidents. | A critical indicator of an organization's ability to quickly and efficiently respond to incidents, minimizing downtime and reducing the impact on operational continuity. A lower MTTRc reflects strong resilience and effective incident response strategies, ensuring that disruptions are short-lived and services are restored promptly. | For customers, a lower MTTRc means reduced downtime and fewer disruptions to their operations, leading to higher satisfaction and trust in the cloud services provided under FedRAMP. For providers, maintaining a low MTTRc demonstrates their commitment to resilience and continuous improvement in their security and operational practices, which can enhance their reputation and competitiveness in the market. This metric also provides transparency to FedRAMP stakeholders, showcasing the provider's ability to maintain service availability and security, thereby strengthening the overall FedRAMP framework. |

| Proposed Metric | Description | Why It Matters | How This Improves the Experience for Customers and/or Providers |
|---|---|---|---|
| ***Incident Dwell Time*** | Measures the total time an attacker remains undetected within a network or system before being identified and removed. | Lower dwell time means that intrusions are being detected and mitigated more quickly, reducing the window of opportunity for attackers. | Shorter dwell times indicate that potential threats are being neutralized quickly, which is critical for maintaining FedRAMP compliance and protecting sensitive government data. Providers that minimize dwell time can reassure customers that their data remains secure and breaches are promptly contained. |
| ***Patch Management Effectiveness*** | The percentage of critical vulnerabilities patched within a defined timeframe (e.g., 30 days) after a patch is released. | Prompt patching of vulnerabilities is key to preventing exploitation by attackers. This metric directly measures the organization's ability to mitigate known risks. | Effective patch management directly contributes to maintaining a secure environment by ensuring that known vulnerabilities are addressed swiftly. For customers, this means that the systems they rely on are less likely to be compromised, reinforcing the integrity of FedRAMP-authorized services. |
| ***Vulnerability Remediation Time*** | The average time taken to remediate vulnerabilities after they have been identified, including through vulnerability scanning or penetration testing. | Shorter remediation times indicate a proactive approach to reducing vulnerabilities and potential attack vectors in the system. | Quick remediation of vulnerabilities ensures that systems remain secure against evolving threats, aligning with FedRAMP's continuous monitoring requirements. Customers benefit from a reduced risk of exploitation, knowing their provider is proactive in maintaining a secure environment. |
| ***Security Event Volume*** | The total number of security events (e.g., attempted logins, firewall blocks, alerts) logged over a specific period. | While not a direct measure of security effectiveness, analyzing trends in security event volume can indicate the level of threat activity and help in resource allocation for security operations. | By tracking and analyzing security event volumes, providers can better allocate resources to address emerging threats, enhancing the overall security posture. Customers gain confidence in the service's resilience, knowing that security events are monitored and managed effectively. |

| Proposed Metric | Description | Why It Matters | How This Improves the Experience for Customers and/or Providers |
|---|---|---|---|
| ***False Positive Rate*** | The percentage of security alerts that are incorrectly flagged as threats. | A high false positive rate can overwhelm security teams and reduce their effectiveness. Monitoring and reducing this rate ensures that security resources are focused on real threats. | Reducing false positives improves the efficiency of security operations by ensuring that genuine threats receive the attention they need. This enhances the accuracy and reliability of security monitoring, which is critical for FedRAMP compliance and gives customers assurance that their provider is focused on real threats. |
| ***User Access Review Frequency and Findings*** | Measures the frequency of access reviews and the number of inappropriate access rights identified and corrected during each review. | Regular access reviews help ensure that users have access to only the data and systems they need, reducing the risk of internal threats and unauthorized access. | Regular access reviews ensure that only authorized personnel have access to sensitive systems, reducing the risk of insider threats. For customers, this metric demonstrates that the provider is vigilant about access controls, aligning with FedRAMP's emphasis on safeguarding sensitive data. |
| ***Phishing Test Success Rate*** | Measures the percentage of employees who successfully identify and report phishing attempts during regular phishing simulations. | Measures the effectiveness of security awareness training and the organization's ability to defend against social engineering attacks. | High success rates in phishing tests indicate effective security awareness among the provider's employees, reducing the risk of social engineering attacks. This enhances customer confidence in the provider's internal security culture and commitment to preventing breaches. |
| ***Rate of Security Incidents Caused by Misconfigurations*** | Measures the percentage of security incidents that can be traced back to system or network misconfigurations. | A lower rate indicates better adherence to security best practices and more rigorous system configuration management, which reduces the likelihood of breaches. | Reducing the number of incidents caused by misconfigurations highlights the provider's competence in maintaining secure system configurations. For customers, this metric demonstrates that the provider's systems are managed according to best practices, reducing the likelihood of avoidable breaches. |

| Proposed Metric | Description | Why It Matters | How This Improves the Experience for Customers and/or Providers |
|---|---|---|---|
| ***Endpoint Detection and Response (EDR) Coverage*** | Measures the percentage of endpoints (e.g., workstations, servers) that are actively monitored and protected by EDR solutions. | High EDR coverage ensures that more potential threats can be detected and responded to across the organization's environment. | Comprehensive EDR coverage ensures that all endpoints are monitored for threats, which is critical for maintaining the security of FedRAMP-authorized systems. Customers can trust that their provider is vigilant in protecting all access points, enhancing overall service security |
| ***Security Patch Failure Rate*** | Measures the percentage of security patches that fail during deployment and require additional remediation efforts. | A lower failure rate indicates more effective and reliable patch management processes, reducing the risk of unpatched vulnerabilities. | A low security patch failure rate indicates robust and reliable patch management processes, reducing the risk of unpatched vulnerabilities. This aligns with FedRAMP's continuous monitoring requirements and reassures customers that their systems are kept secure and up to date. |
| ***Data Exfiltration Detection Rate*** | The percentage of attempted data exfiltration events that are successfully detected and blocked. | Directly measures the effectiveness of data loss prevention controls and the organization's ability to protect sensitive information. | High detection rates of data exfiltration attempts are crucial for protecting sensitive government data, a key focus of FedRAMP. Providers that excel in this area offer customers strong assurance that their data is safeguarded against unauthorized transfers. |
| ***Backup and Recovery Testing Frequency*** | Measures the frequency of testing backup and recovery processes and the success rate of those tests. | Regular and successful testing of backups ensures that the organization can recover from data loss incidents, minimizing downtime and data loss. | High detection rates of data exfiltration attempts are crucial for protecting sensitive government data. FedRAMP Improvement: Regular and successful backup and recovery tests ensure data availability and integrity, even in the event of a security incident. For customers, this metric demonstrates that their provider has robust disaster recovery capabilities, which is a critical component of FedRAMP's risk management framework. |

| Proposed Metric | Description | Why It Matters | How This Improves the Experience for Customers and/or Providers |
|---|---|---|---|
| ***Secure Configuration Compliance Rate*** | Measures the percentage of systems that adhere to predefined secure configuration baselines (e.g., Center for Internet Security benchmarks). | Ensuring systems are configured securely reduces the attack surface and prevents exploitation of misconfigured systems. | Maintaining a high rate of compliance with secure configuration standards ensures that the provider's systems are resilient against threats. This is essential for FedRAMP compliance and gives customers confidence that the systems they rely on are configured according to stringent security standards. |

## Rethinking FedRAMP Continuous Monitoring Metrics to Improve National Security

Today's FedRAMP continuous monitoring requirements call for CSPs to report known vulnerabilities every 30 days and security incidents within an hour.[7,8,9] While these are reasonable target objectives, it is not clear that they effectively support national cyber defense. First, vulnerabilities are important only if an adversary can exploit them. Second, CSPs can easily get lost in the plethora of security messages generated by today's IT systems and event analysis can take many hours to days and even months to attribute events to malicious actors.

The CSFT recommends that continuous monitoring approaches be advanced to include more real-time measures of cloud security health and malicious activity in order to provide a better understanding of CSP cyber risk. As government adoption of cloud services increases, the adversary follows.[10,11] Significant portions of adversarial behavior are now seen firsthand by CSPs. As a result, the dominant U.S. CSPs now possess an excellent vantage point from which to monitor and report adversary activity. It is reasoned that CSPs could be called to track and report known adversary or malicious actor behavior in more real time. Such tracking can discover adversary targets and exploitation methods. If reporting of associated observable data is performed in timely manner, cloud consumers could better prepare and take protective measures. Ensuring adversaries do not simply adjust tactics, techniques, and procedures (TTPs) based on the measurements put in place will require careful management and balance. The following table provides a list of suggested metrics to help FedRAMP better drive improvements to national security.

[7] FedRAMP Training - Continuous Monitoring (ConMon) Overview. 2015. FedRAMP, https://www.fedramp.gov/assets/resources/training/200-D-FedRAMP-Training-Continuous-Monitoring-ConMon-Overview.pdf.

[8] FedRAMP Continuous Monitoring Performance Management Guide. 2023. FedRAMP, https://www.fedramp.gov/assets/resources/documents/CSP_Continuous_Monitoring_Performance_Management_Guide.pdf.

[9] FedRAMP Incident Communications Procedures. 2021. FedRAMP, https://www.fedramp.gov/assets/resources/documents/CSP_Incident_Communications_Procedures.pdf.

[10] 2024 Threat Detection Report. 2024. Red Canary, https://redcanary.com/threat-detection-report. Last Accessed August 22, 2024.

[11] M-Trends 2024 Special Report. 2024. Google Cloud Security, https://services.google.com/fh/files/misc/m-trends-2024.pdf.

| Metric and Description | Objective | Benefit to Government | Benefit to Industry |
|---|---|---|---|
| ***Real-Time Vulnerability Exploitation Risk Score:*** Assesses the likelihood and potential impact of known vulnerabilities being exploited by adversaries in real-time. This score would be calculated based on factors such as the severity of the vulnerability, the presence of known adversaries targeting similar vulnerabilities, and the current state of the CSP's defenses. | To prioritize vulnerabilities based on actual exploitation risk rather than simply their presence, enabling more effective and timely mitigation efforts. | Allows for more strategic allocation of resources by prioritizing vulnerabilities that are most likely to be exploited, improving national cyber defense and reducing unnecessary focus on low-risk issues. | Enhances the ability to focus on critical vulnerabilities, reducing the time and resources spent on less significant issues and improving overall security effectiveness. |
| ***Zero-Day Exploit Detection and Mitigation Index:*** Measures an organization's effectiveness in detecting, responding to, and mitigating zero-day exploits. The index is calculated by evaluating the speed of detection, the integration of threat intelligence, the responsiveness of incident management processes, and the adaptability of the organization's defenses to new and unknown threats. | To prioritize and enhance an organization's capability to swiftly identify and neutralize zero-day threats, ensuring proactive mitigation efforts that minimize the impact of such exploits before they can cause significant harm. | Strengthens national cybersecurity by ensuring that critical public-sector systems are equipped to handle emerging threats. Enhances the government's ability to protect sensitive data and infrastructure from unknown vulnerabilities, thereby safeguarding national security. Promotes a more robust and resilient national defense posture against sophisticated cyber threats, reducing potential risks to public safety and continuity of government operations. | Encourages the development and adoption of advanced detection and mitigation technologies, fostering innovation within the cybersecurity sector. Helps businesses minimize the risk of zero-day exploits, reducing potential financial losses, reputational damage, and operational disruptions. Enables companies to align their cybersecurity strategies with best practices, ensuring they remain competitive and compliant with evolving security standards and regulations. |
| ***Adversarial Behavior Detection and Reporting Time:*** The elapsed time from detection of confirmed adversarial activity to the reporting of this activity to relevant stakeholders, | To ensure timely awareness and response to potential threats, reducing the window of opportunity for adversaries to | Provides earlier warnings of potential threats, allowing for quicker decision making and deployment of defensive measures to protect national infrastructure. | Improves the trust and reliability of the provider's services by demonstrating a commitment to rapid threat detection and communication, potentially reducing |

| Metric and Description | Objective | Benefit to Government | Benefit to Industry |
|---|---|---|---|
| including cloud consumers and government agencies. | exploit vulnerabilities. | | the impact of incidents and enhancing customer relationships. |
| ***Real-Time Security Event Correlation Rate:*** The percentage of security events that are correlated in real time with known adversarial patterns or behavior. This includes events that are automatically flagged as suspicious based on historical data or threat intelligence. | To improve the accuracy and speed of identifying genuine threats among the large volume of security events, thereby enhancing the CSP's ability to respond to real attacks. | Increases the precision of threat intelligence, leading to more accurate and timely responses to potential threats, enhancing overall national security posture. | Reduces noise from false positives, enabling security teams to focus on genuine threats, improving operational efficiency and reducing costs associated with incident response. |
| ***Adversary Activity Engagement Frequency:*** The frequency at which CSPs are able to track observed adversarial activities or patterns, potentially on a daily, hourly, or near-real-time basis. | To provide continuous visibility into adversarial activities, enabling cloud consumers and national security agencies to stay informed and take preemptive actions. | Ensures that CSP providers are gaining continuous insight into the threat landscape, allowing for ongoing adjustments to security policies and strategies in real time. | Demonstrates a proactive security stance to customers and regulators, potentially improving market reputation and trust, while also aligning with compliance requirements. |
| ***Adversary Target Identification Rate:*** The rate at which CSPs identify and confirm potential targets of adversarial interest within their infrastructure, including specific cloud services or data sets. | To allow for proactive defense measures, such as increased monitoring or enhanced security controls, around identified targets. | Helps in identifying critical national assets that are under threat, enabling focused protection efforts and better-informed policymaking. | Allows for targeted security measures around high-risk areas, potentially preventing successful attacks and reducing the likelihood of severe security breaches. |
| ***Exploitation Method Discovery Time:*** The time taken to discover and document new exploitation methods used by adversaries, from initial detection to full analysis and reporting. | To reduce the time window in which adversaries can utilize new methods undetected, thereby improving the overall security posture of the cloud environment. | Reduces the time adversaries have to exploit new vulnerabilities, helping protect critical national infrastructure from emerging threats. | Accelerates the implementation of countermeasures against new attack methods, reducing the potential for damage and associated remediation. |

| Metric and Description | Objective | Benefit to Government | Benefit to Industry |
|---|---|---|---|
| ***Consumer Protective Action Lead Time:*** The time available for cloud consumers to take protective measures after receiving a report on adversarial activity or vulnerabilities, before potential exploitation occurs. | To ensure that cloud consumers have sufficient time to respond effectively to threats, minimizing the impact of potential security incidents. | Ensures that government agencies and critical infrastructure providers have sufficient time to defend against threats, minimizing the impact of attacks on national security. | Enhances customers' satisfaction and trust by providing them with ample time to implement protective measures, thereby reducing the likelihood of successful attacks and associated liabilities. |
| ***Security Incident Attribution Accuracy:*** The accuracy with which security incidents are attributed to specific adversaries or malicious actors, based on the analysis of event data and threat intelligence. | To improve the precision of incident response efforts by accurately identifying the source of threats, thereby enabling targeted and effective countermeasures. | Improves the ability to hold the correct adversaries accountable, enabling more targeted and effective responses to cyber threats, including sanctions or retaliatory actions. | Increases the precision of threat mitigation efforts, reducing the chances of incorrectly targeting benign activities and improving the overall effectiveness of incident response. |

## Rethinking FedRAMP Continuous Monitoring with Continuous Testing

Adversaries target our IT systems relentlessly, finding vulnerabilities and executing exploitation routines before we even recognize there is a problem. The recent Mandiant 2024 M-Trends Report indicates that Zero-Day vulnerabilities—previously unknown vulnerabilities that are exploited before developers have a chance to address them—has increased from previous years.[12] While improved coding methods would help, software vendors do not invest the time and effort necessary to produce vulnerability-free code. As a result, software that goes into production possess a technical debt that can compromise government systems and sensitive data. Today, the cyber battlefield is asymmetric, and adversaries are targeting and benefiting from our software technical debt. The only reasonable defense in today's cyber battle environment is to proactively find our own vulnerabilities before adversaries do.

Red and Blue teaming activities need not be performed only at single points in time, such as during assessment and authorization. They can be conducted much more routinely and even continuously. In addition, cyber assessment against known and emerging vulnerabilities can be automated. For example, the MITRE SAF solution provides automation in the Development, Security, and Operations (DevSecOps) pipeline[13] and the MITRE Caldera tool can be used for automating adversary attack behaviors.[14] Cybersecurity businesses specializing in these areas have emerged, and their practices have become considerably more efficient and effective. In fact, some FedRAMP-certified 3PAOs are believed to possess both Red and Blue teaming

[12] M-Trends 2024 Special Report.

[13] MITRE Security Automation Framework. 2024. MITRE, https://saf.mitre.org/. Last accessed August 27, 2024.

[14] MITRE CALDERA. 2024. MITRE, https://caldera.mitre.org/. Last accessed August 27, 2024.

capabilities. Given the technical debt in which our systems are deployed today, this industry is considered underutilized.

To foster a continuous testing mentality among CSPs, FedRAMP could institute metrics that measure the extent of Red and Blue teaming performed by CSPs. Metrics could include measures of the number of Zero-Day exploits discovered, the number of successful Red Team intrusions occurred, the number of employees duped by mock phishing attacks, and so one. The following table provides a list of metrics FedRAMP might employ to enhance continuous testing.

| Metric and Description | Objective | Benefit to Government | Benefit to Industry |
|---|---|---|---|
| ***Frequency of Red and Blue Team Exercises:*** The number of Red and Blue team exercises conducted by CSPs over a defined period (e.g., quarterly or annually). | To assess the regularity of security testing practices aimed at identifying vulnerabilities before adversaries can exploit them. | Ensures that CSPs are consistently testing their defenses, leading to a more secure environment for government systems and data. | Encourages ongoing improvement in security postures, helping CSPs stay ahead of emerging threats and improve their resilience. |
| ***Number of Zero-Day Vulnerabilities Discovered by Red Teams:*** The total number of Zero-Day vulnerabilities discovered by Red Team activities within a specified timeframe. | To measure the effectiveness of proactive security testing in uncovering critical vulnerabilities before they can be exploited by adversaries. | Reduces the risk of Zero-Day exploits affecting federal systems by ensuring vulnerabilities are identified and mitigated early. | Helps CSPs identify and fix critical flaws in their systems, reducing potential damage from unforeseen attacks and enhancing their security reputation. |
| ***Success Rate of Red Team Intrusions:*** The percentage of Red Team exercises that result in successful intrusions or breaches, measured against the total number of exercises conducted. | To evaluate the effectiveness of existing security measures and identify areas where defenses may be lacking. | Provides insight into the robustness of CSP security, ensuring that federal data is protected by effective defenses. | Offers valuable feedback on security weaknesses, allowing CSPs to improve their defensive strategies and reduce the likelihood of real-world breaches. |
| ***Number of Employees fooled by Mock Phishing Attacks:*** The number of CSP employees who fall victim to mock phishing campaigns conducted as part of Blue Team activities. | To assess the effectiveness of security awareness training and identify potential insider risks. | Enhances the overall security posture by ensuring that CSP personnel are well trained and aware of common attack vectors. | Encourages CSPs to invest in employee training, reducing the risk of successful phishing attacks and improving overall security culture. |
| ***Time to Remediate Vulnerabilities Identified by Red and Blue Teams:*** The average time taken by CSPs to remediate vulnerabilities | To measure the responsiveness of CSPs in addressing discovered | Reduces the window of opportunity for adversaries to exploit vulnerabilities, protecting federal | Demonstrates a commitment to rapid vulnerability management, enhancing the trust of |

| Metric and Description | Objective | Benefit to Government | Benefit to Industry |
|---|---|---|---|
| identified during Red and Blue team exercises. | vulnerabilities, ensuring swift action to mitigate risks. | systems from potential breaches. | government clients and improving service reliability. |
| ***Cost Savings from Proactive Vulnerability Identification:*** The estimated cost savings achieved by CSPs and the government through the identification and remediation of vulnerabilities before they are exploited by adversaries. | To quantify the financial benefits of proactive security practices, emphasizing the value of continuous Red and Blue teaming. | Illustrates the economic efficiency of investing in continuous testing, justifying budget allocations for security initiatives. | Highlights the cost-effectiveness of maintaining strong security practices, potentially attracting more clients and reducing the financial impact of breaches. |
| ***Percentage of Critical Systems Tested Using Red and Blue Teams:*** The proportion of critical systems within a CSP's environment that undergo regular Red and Blue team testing. | To ensure that the most sensitive and critical systems are consistently tested for vulnerabilities. | Ensures that high-priority systems receive the attention needed to maintain their security and integrity. | Helps CSPs focus their security efforts on the most important systems, minimizing the risk of catastrophic breaches. |
| ***Number of Mitigations Implemented Following Red and Blue Team Findings:*** The total number of security mitigations or improvements implemented as a direct result of Red and Blue team findings. | To measure the impact of continuous testing on the security posture of CSPs. | Demonstrates the effectiveness of proactive security testing in driving tangible security improvements, thus enhancing the protection of federal data. | Provides a clear metric for security advancements, helping CSPs demonstrate their commitment to maintaining high-security standards to their clients. |

## Rethinking FedRAMP Metrics to Support Adoption of Quantum Resistant Cryptography and Zero Trust Initiatives

To keep FedRAMP a strong and dependable framework for securing cloud services within the federal government, it is essential to continuously evolve in line with emerging government and industry best practices. As new needs like the migration to quantum-safe cryptography and new paradigms like Zero Trust Architectures gain prominence, FedRAMP must proactively plan for their integration to address evolving security challenges. Additionally, incorporating a Cryptographic Bill of Materials can provide transparency regarding the cryptographic algorithms used in software, aligning with industry trends. This forward-thinking strategy will not only bolster the security of federal systems but also ensure that FedRAMP remains relevant and effective in a rapidly changing cybersecurity landscape. The following table outlines metrics that FedRAMP could use to strengthen quantum resistant cryptography and Zero Trust tenants.

| Metric and Description | Objective | Benefit to Government | Benefit to Industry |
|---|---|---|---|
| ***Percentage of CSPs Implementing Post-Quantum Cryptographic Algorithms:*** The proportion of FedRAMP-authorized CSPs that have implemented or are in the process of implementing post-quantum cryptographic algorithms to secure their services. | To assess the adoption rate of post-quantum cryptographic measures among CSPs, ensuring preparedness against future quantum-based threats. | Enhances the security posture of federal cloud services by ensuring they are resilient against potential quantum computing threats, thus protecting sensitive government data. | Positions CSPs as leaders in cutting-edge security practices, increasing trust and marketability among government and private-sector clients concerned about future-proofing their data security. |
| ***Time to Implement Post-Quantum Cryptographic Solutions:*** The average time it takes for CSPs to implement post-quantum cryptographic solutions after they are identified as necessary for compliance with evolving FedRAMP standards. | To measure the responsiveness of CSPs in integrating post-quantum cryptography into their services, reflecting their agility in adapting to new security requirements. | Ensures that federal agencies can rely on CSPs to quickly adapt to emerging security standards, minimizing exposure to quantum-based threats. | Encourages CSPs to enhance their operational readiness and responsiveness, which can be a competitive advantage in the rapidly evolving cybersecurity landscape. |
| ***Adoption Rate of Zero Trust Architecture Among FedRAMP-Authorized CSPs:*** The percentage of FedRAMP-authorized CSPs that have adopted Zero Trust Architecture principles in their CSOs. | To evaluate the level of implementation of Zero Trust principles among CSPs, ensuring that security measures are robust and aligned with current best practices. | Improves the security of federal systems by ensuring that CSPs employ a "never trust, always verify" approach, reducing the risk of unauthorized access and breaches. | Demonstrates a commitment to advanced security practices, enhancing the reputation and trustworthiness of CSPs in the eyes of both government and private-sector clients. |
| ***Percentage of Federal Systems Transitioned to Zero Trust Architecture:*** The proportion of federal systems hosted by FedRAMP-authorized CSPs that have transitioned to a Zero Trust Architecture. | To track the progress of federal agencies in moving their systems to a Zero Trust model, ensuring alignment with modern security frameworks. | Facilitates a more secure federal IT environment by ensuring that critical systems are protected by modern, robust security architectures. | Encourages CSPs to develop and offer Zero Trust–compliant services, opening up new market opportunities as agencies seek to meet evolving security mandates. |

# Recommended Edits to Proposed Metrics

## Metric #1: Assessment - 3PAO Time & Cost

This metric tracks the total time and overall cost required for a FedRAMP-recognized 3PAO to conduct various assessments, including:

- New Initial Assessments
- Annual Assessments
- Readiness Assessments

Key considerations include:

- Is this truly beyond the FedRAMP Program Management Office's (PMO's) control given that FedRAMP sets the requirements for these assessments?
- Does FedRAMP exercise any oversight or quality control over 3PAOs? This should be considered at least a shared responsibility, especially given the significant impact that 3PAOs can have on the experience of CSPs and agencies going through the FedRAMP process.
- Beyond the size and scope of the assessment, other factors to consider include the number of staff hours 3PAOs allocate to a given assessment, the assessors' expertise and familiarity with the specific CSO/technology, and the assessors' experience in performing such assessments.

## Metric #11: Package Resubmission

This metric measures the number of times a CSP resubmits a package for FedRAMP review to obtain initial authorization. However, several questions arise:

- How or why is this considered a "security" metric? It appears more related to the FedRAMP process and the user experience for CSPs. What does this metric say about the actual security of a CSO after undergoing FedRAMP?
- Without understanding the reasons behind the resubmissions, what can this metric reveal? For example, resubmissions could result from deficiencies in package artifacts, processing errors by reviewers, or inadequate implementation of specific security controls.

These points suggest that while these metrics may provide some insights, they need to be interpreted carefully to ensure they are genuinely contributing to an understanding of security effectiveness and not merely reflecting process inefficiencies.

# Answers to "RFI Question to Consider"

## 1. In your opinion, what are the most important metrics for assessing the efficiency and effectiveness of the FedRAMP process and how can FedRAMP ensure we are getting an accurate representation of this data when collected?

To evaluate the effectiveness of the FedRAMP process and ensure that the collected data accurately reflects its impact, MITRE has adopted a holistic approach. This involves assessing the overall influence of the metrics used in FedRAMP and identifying strategies to achieve better outcomes. The following table provides our answers to the question posed, accompanied by additional context and rationale for improving the entire overall process. This integrated approach aims to enhance the accuracy of data representation and drive meaningful improvements in the FedRAMP framework.

| Area of Focus | Definition | Importance | Ensuring Accuracy |
|---|---|---|---|
| ***1. Time to Authorization (TTA)*** | The time it takes for a CSP to go through the entire FedRAMP process, from initial submission to obtaining authorization. | Reflects the efficiency of the FedRAMP process. A shorter TTA indicates a more streamlined process, while longer times may suggest bottlenecks or inefficiencies. | Track the TTA across various types of Cloud Service Providers (CSPs) (e.g., Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS)) and by authorization type (e.g., Joint Authorization Board (JAB) Provisional Authorization, Agency Authorization). Implement consistent definitions for process milestones and ensure that data is collected at each stage. |
| ***2. Authorization Success Rate*** | The percentage of CSPs that successfully obtain FedRAMP authorization out of those that start the process. | A high success rate may indicate that the FedRAMP requirements are clear and achievable, whereas a low rate could suggest barriers to entry or unclear guidelines. | Compare success rates across different CSP sizes and types. Conduct post-authorization surveys to gather feedback on challenges faced during the process. |
| ***3. Cost of Authorization*** | The total cost incurred by CSPs and the government during the authorization process, including labor, consultancy, and resource allocation. | Critical for assessing the economic efficiency of the FedRAMP process. The metric helps determine whether the cost burden is justifiable for the level of security assurance provided. | Require standardized cost reporting from CSPs and federal agencies, ensuring that costs are broken down into categories like initial assessment, ongoing compliance, and reauthorization. |

| Area of Focus | Definition | Importance | Ensuring Accuracy |
|---|---|---|---|
| ***4. Security Incident Rate Post-Authorization*** | The frequency of security incidents reported by authorized CSPs after they have been authorized by FedRAMP. | Evaluates the effectiveness of the FedRAMP process in ensuring that only secure CSPs receive authorization. A low incident rate would indicate a strong vetting process, while a higher rate could suggest the need for tighter controls or better monitoring. | Implement mandatory reporting of security incidents for FedRAMP-authorized CSPs. Cross-reference this data with broader federal cybersecurity incident databases to validate completeness. |
| ***5. Customer Satisfaction (Federal Agencies)*** | The satisfaction level of federal agencies that utilize FedRAMP-authorized services, often measured through surveys. | Provides insight into how well FedRAMP meets the needs of its primary users. High satisfaction levels indicate that the services meet security, usability, and performance expectations. | Regularly conduct and update surveys post-implementation of cloud services. Include qualitative feedback to capture nuanced issues and opportunities for improvement. |
| ***6. Reauthorization and Continuous Monitoring Metrics*** | The frequency and outcomes of reauthorization and continuous monitoring activities. | Continuous monitoring and periodic reauthorization are crucial for maintaining long-term security and compliance. Effective monitoring ensures that CSPs remain compliant after their initial authorization. | Standardize the reporting process for continuous monitoring activities, ensuring consistent data collection across different CSPs. Monitor the timeline and outcomes of reauthorization processes to identify trends and areas for improvement. |
| ***7. Stakeholder Engagement and Feedback*** | The level of engagement and feedback from stakeholders, including CSPs, federal agencies, and 3PAOs. | Effective communication and feedback loops are crucial for adapting and improving the FedRAMP process. High engagement suggests that stakeholders are invested in the process and see value in it. | Regularly gather and analyze feedback through workshops, forums, and surveys. Ensure that all stakeholder groups are represented and that their concerns are addressed in policy updates. |
| ***8. Time-to-Resolve Plan of Action and Milestones (POAM)*** | Open POAM issues should be resolved in a timely manner. Tracking the time to remediate for POAM issues provides a | POAM issues that remain open for extended periods of time indicate a problem in assessment or control specifications. | CSPs can and should be required to report the status of POAM issues. Closure reports should be validated by the FedRAMP PMO. CSPs could submit POAM |

| Area of Focus | Definition | Importance | Ensuring Accuracy |
|---|---|---|---|
| | measure of assessment effectiveness. Measures the difference between the predicted resolution date and the actual date. | Additionally, implicated vulnerabilities leave cloud systems exposed to adversary behavior. | status/resolution metrics and FedRAMP should validate and confirm to ensure accuracy. |

## 2. What role could FedRAMP play in helping define success regarding timeliness and cost effectiveness of the authorization process where FedRAMP is not involved in every phase of the authorization process?

FedRAMP can play a critical role in defining success regarding the timeliness and cost-effectiveness of the authorization process, even in phases where it is not directly involved. This can be achieved through several strategies focused on guidance, standardization, oversight, and continuous improvement. By establishing clear benchmarks and best practices, FedRAMP can ensure that the entire authorization process, from start to finish, meets high standards of efficiency and effectiveness. These efforts can help streamline the process, reduce costs, and improve the overall experience for CSPs and government agencies alike.

The following table outlines specific strategies and metrics that FedRAMP could implement to define and measure success in terms of timeliness and cost-effectiveness throughout the authorization process.

| Topic | Role | Impact |
|---|---|---|
| ***1. Continue Providing Clear and Detailed Guidelines*** | FedRAMP can continue to set clear expectations and provide detailed guidelines for all parties involved in the authorization process, including CSPs, agencies, and 3PAOs. These guidelines should outline best practices for timeliness and cost management throughout the process. A continual engagement approach to clarifying changes to metrics will be essential. | By setting clear expectations, FedRAMP helps ensure that all stakeholders understand the steps required to achieve authorization efficiently, which can reduce delays and prevent unnecessary expenses. |
| ***2. Establishing Performance Benchmarks*** | FedRAMP can define and publish performance benchmarks for each phase of the authorization process, including those not directly overseen by FedRAMP. These benchmarks can include average timeframes for each phase, cost expectations, and assessment of the difficulty in achieving compliance with specific security controls. | Benchmarks provide a reference point for all parties, allowing them to assess their performance against industry standards. This transparency encourages accountability and motivates stakeholders to meet or exceed the established benchmarks. |
| ***3. Promoting Best Practices and Lessons Learned*** | FedRAMP can collect and disseminate best practices and lessons learned from past authorizations, including feedback on what worked well in terms of timeliness | By promoting best practices, FedRAMP enables stakeholders to adopt strategies that have been proved to reduce time and |

| Topic | Role | Impact |
|---|---|---|
| | and cost management. This information can be shared through training sessions, workshops, and documentation. | costs, leading to more efficient authorization processes. |
| ***4. Facilitating Collaboration Among Stakeholders*** | FedRAMP can foster collaboration among CSPs, federal agencies, and 3PAOs by creating forums, working groups, and partnerships that encourage sharing information and strategies for improving efficiency and security. This collaboration can also help identify and address common bottlenecks in the process. | Enhanced collaboration leads to a more coordinated approach to authorization, reducing misunderstandings, duplicative efforts, and delays, thereby improving both timeliness and cost-effectiveness. |
| ***5. Monitoring and Reporting on Timeliness and Costs*** | Even if FedRAMP is not involved in every phase, it can monitor and collect data on the timeliness and costs associated with the entire authorization process. This could include post-authorization surveys or regular reporting requirements for CSPs and agencies. | By tracking this data, FedRAMP can identify trends, highlight areas for improvement, and provide targeted guidance to improve future processes. This data-driven approach ensures that any inefficiencies are addressed, even in phases outside of direct FedRAMP oversight. |
| ***6. Implementing a Continuous Feedback Loop*** | FedRAMP can establish a continuous feedback loop where stakeholders provide input on the challenges they face in terms of timeliness and cost during the authorization process. This feedback can be used to refine the process and update guidelines and benchmarks as necessary. | Continuous improvement ensures that the authorization process evolves to meet the changing needs of stakeholders, leading to more efficient and cost-effective outcomes over time. |
| ***7. Standardizing 3PAO and Agency Assessment Practices*** | FedRAMP can work with 3PAOs and federal agencies to standardize assessment practices, reducing variability in the time and cost associated with different assessments. This includes providing templates, checklists, and standardized tools that all assessors can use. | Standardization reduces the risk of delays due to inconsistent practices and helps ensure that all parties are working toward the same objectives, ultimately improving both timeliness and cost-effectiveness. |
| ***8. Incentivizing Timeliness and Cost Efficiency*** | FedRAMP can create incentives for CSPs, agencies, and 3PAOs that demonstrate exceptional performance in terms of timeliness and cost management. This could include recognition programs, expedited reviews for future authorizations, or other benefits. | Incentives encourage stakeholders to prioritize efficiency and cost management, leading to a more streamlined authorization process. |
| ***9. Regularly Reviewing and Updating Authorization Requirements*** | FedRAMP can periodically review and update its authorization requirements to ensure they are aligned with current technologies and industry practices. Simplifying or refining these requirements can reduce the time and cost associated with compliance. | Regular updates prevent the process from becoming overly burdensome or outdated, helping maintain efficiency and cost-effectiveness. |

| Topic | Role | Impact |
|---|---|---|
| ***10. Providing Transparency in Costs*** | FedRAMP can provide transparency into the cost structures associated with different phases of the authorization process, helping CSPs and agencies budget more accurately and identify areas where costs can be reduced. | Transparency in costs helps all stakeholders plan more effectively, reducing the likelihood of cost overruns and ensuring a more efficient use of resources. |

## 3. What types of information would help to manage your expectations and improve your experience during the FedRAMP authorization process?

The following table provides specific types of information and strategies that could help manage expectations and improve the experience for Cloud Service Providers (CSPs) during the FedRAMP authorization process.

| Area for Focus | Details | Impact |
|---|---|---|
| ***1. Clear Process Roadmap*** | A detailed, step-by-step roadmap of the FedRAMP authorization process, including key milestones, required documentation, and expected timelines for each phase. | Helps stakeholders understand the full scope of the process, allowing them to plan resources and timelines accordingly. |
| ***2. Estimated Timelines*** | Realistic estimates for how long each stage of the authorization process is expected to take, based on historical data and specific factors related to the project (e.g., complexity of the system, chosen pathway, implementation approach). | Provides a clear expectation of the time commitment required, helping align project timelines and manage expectations within the organization. |
| ***3. Cost Breakdown*** | A breakdown of the typical costs associated with each phase of the FedRAMP process, including third-party assessments, internal resource allocation, and potential unexpected expenses. | Helps in budgeting and financial planning, ensuring that stakeholders are prepared for the financial aspects of the authorization process. |
| ***4. Roles and Responsibilities*** | Clear definitions of the roles and responsibilities of all parties involved in the FedRAMP process, including CSPs, federal agencies, 3PAOs, and the FedRAMP PMO. | Clarifies who is responsible for what, reducing confusion and ensuring that all parties are aligned and accountable throughout the process. |
| ***5. Common Challenges and Mitigation Strategies*** | Information on common challenges encountered during the FedRAMP process, along with recommended mitigation strategies and best practices for | Prepares stakeholders for potential roadblocks and provides actionable strategies to overcome them, improving overall efficiency. |

| Area for Focus | Details | Impact |
|---|---|---|
| | avoiding delays and additional costs. | |
| ***6. Access to Resources and Tools*** | Access to tools, templates, and resources that support the FedRAMP process, such as documentation templates, automated compliance tools, and a knowledge base of frequently asked questions. | Provides practical support to help streamline the process and reduce administrative burden on the stakeholders involved. |
| ***7. Regular Updates and Communication*** | Regular updates on the progress of the authorization process, including any changes to timelines, requirements, or other critical information. | Keeps all stakeholders informed and engaged, reducing uncertainty and helping maintain momentum throughout the process. |
| ***8. Feedback Mechanisms*** | Mechanisms for providing feedback and asking questions throughout the process, ensuring that concerns are addressed promptly and that the process is continually improved based on stakeholder input. | Enhances the user experience by allowing for real-time communication and problem-solving, making the process more responsive to the needs of those involved. |
| ***9. Success Stories and Case Studies*** | Case studies or success stories from other organizations that have successfully navigated the FedRAMP process, highlighting the benefits achieved and lessons learned. | Provides motivation and practical insights that can guide the current process, helping stakeholders see the value and end goal of the authorization effort. |
| ***10. Expected Outcomes and Metrics*** | Clear metrics and outcomes that define what success looks like at each stage of the process, including security benchmarks, compliance milestones, and final authorization deliverables. | Helps stakeholders understand what they need to achieve at each stage, ensuring that efforts are focused on meeting the necessary criteria for success. |

The CSTF has identified a significant issue with the responsiveness of the FedRAMP PMO to CSP inquiries related to assessment and authorization processes. Slow or inaccurate responses to these inquiries can lead to increased costs and uncertainty for CSPs, potentially disrupting their business operations.

To address this, we propose that the FedRAMP PMO establish an Information Desk supported by an inquiry ticketing system. This system would track information requests, providing real-time ticket status updates and detailed closure metrics. Additionally, ticket closure rates and post-engagement satisfaction surveys could offer valuable insights into the FedRAMP PMO's responsiveness and the usefulness of the information provided. Implementing such a system would not only enhance transparency but also help ensure that CSPs receive timely and accurate support, ultimately improving the overall efficiency of the FedRAMP process.

## 4. Do you use specific performance metrics within your organization to monitor progress that you feel would be a good standard to share with other FedRAMP?

While MITRE has established internal performance metrics tailored to our unique organizational needs, we believe that the most effective metrics are those that are customized to an organization's specific goals and context. We encourage others to develop and refine metrics that align closely with their own operational priorities and the unique demands of their FedRAMP engagements.

## 5. How confident are you in the quality and completeness of the data you will provide for these metrics? What measures do you think could improve the accuracy and reliability of the data?

While the above set of considerations and changes could significantly improve the accuracy, reliability, and usability of the overall FedRAMP process, additional ideas and concepts could further enhance the outcomes sought as part of the changes to the FedRAMP system of measurements and metrics. We believe the additional ideas in the table below will provide further levels of detail about the efficacy of the program:

| Concept | How It Works | Impact |
|---|---|---|
| ***1. Innovation Impact Metric:*** Assess how the FedRAMP process impacts innovation within CSPs and across federal agencies. | Track the introduction of new services, features, or technologies by CSPs before, during, and after FedRAMP authorization. Measure the time to market for innovative features post-authorization and how agencies adopt these innovations. | This metric would help FedRAMP understand whether its process is enabling or stifling innovation. It could also provide insights into how the process might be adapted to better support the rapid evolution of technology. |
| ***2. Security Improvement Over Time:*** Instead of assessing security only at a point in time (during authorization), this metric would track how a CSP's security posture improves over time as a direct result of the FedRAMP process. | Continuously monitor and compare the security incidents, vulnerability resolution times, and security audit results of CSPs before, during, and after FedRAMP authorization. | This metric would highlight the long-term benefits of the FedRAMP process, showing how it contributes to ongoing security improvements, rather than being a one-time compliance exercise. |
| ***3. Customer Value Perception Index:*** Measure how federal agencies perceive the value of FedRAMP-authorized CSPs in terms of cost, performance, security, and overall satisfaction. | Conduct surveys and collect data from agencies using FedRAMP-authorized services to assess how well these services meet their needs and how they compare to non-authorized alternatives. | This metric would provide insight into the real-world value of FedRAMP authorization from the end-users' perspective, potentially influencing how the process is marketed or refined. |

| Concept | How It Works | Impact |
|---|---|---|
| ***4. Cross-Agency Collaboration Metric(s) (CACM):*** Evaluate the level of collaboration between federal agencies during the FedRAMP authorization process and the shared use of FedRAMP-authorized solutions. | Track the number of agencies that collaboratively work on a single FedRAMP authorization or share the same CSP service and measure the frequency and effectiveness of interagency communications and decisions. | A high CACM score could indicate that FedRAMP is effectively fostering collaboration across the government, leading to more consistent and streamlined use of cloud services. |
| 5. ***Ecosystem Resilience Metric(s):*** Assess how resilient the FedRAMP ecosystem is to changes, such as new security threats, policy changes, or technological advancements. | Measure the speed and effectiveness with which FedRAMP-authorized CSPs and the FedRAMP program itself can adapt to new challenges. This could include tracking the time taken to implement new security controls in response to emerging threats or the adoption rate of new guidelines. | This metric would provide insights into how robust and flexible the FedRAMP process is, ensuring it can remain effective in a rapidly changing environment. |
| ***6. End-to-End Lifecycle Cost Efficiency (ELCE):*** Move beyond the initial cost of authorization and measure the total lifecycle cost efficiency of maintaining FedRAMP authorization, including continuous monitoring and reauthorization. | Track all associated costs from initial authorization through the lifecycle of the CSP's service, including ongoing compliance costs, resource allocation for continuous monitoring, and any costs associated with reauthorization. | ELCE would provide a more comprehensive understanding of the financial implications of FedRAMP over time, helping CSPs and agencies budget more effectively and identify opportunities for cost savings. |

# Conclusion

In this RFI response, MITRE leverages its many years of experience working with the U.S. government and the cloud services industry to deliver security solutions for government cloud adoption consistent with MITRE's ECAF. Timely and relevant experience derived from MITRE's involvement in the Cloud Safe Task Force has also been brought to bear in answering this RFI.

Therefore, the MITRE-led CSTF makes recommendations designed to enhance FedRAMP's purpose of accelerating cloud adoption, ensuring the security of critical national digital assets, and encouraging innovation and greater availability of evolving cloud services by rethinking FedRAMP's measures of:

- **Processes and Metrics to Drive Reciprocity**: Introducing RaS to reduce redundant assessments and streamline compliance across different frameworks
- **Measures of Effectiveness**: Transitioning to continuous monitoring with real-time and resilience-based cyber performance metrics to enhance security effectiveness

- **Continuous Monitoring Metrics**: Advancing continuous monitoring to include real-time measures of cloud security health and adversary activity
- **Continuous Testing**: Promoting continuous Red and Blue teaming activities and automated cyber assessments to proactively identify vulnerabilities
- **Support for Quantum Resistant Cryptography and Zero Trust Initiatives**: Integrating forward-thinking strategies to address emerging security challenges
- **Measuring Reciprocity as an Indicator of Industry Cost of Authorization**: Evaluating the extent of reassessments required for FedRAMP Provisional Authorization to reduce costs and improve efficiency

MITRE acknowledges that the proposed metrics and recommendations are in draft form and may require further refinement. However, they provide a solid foundation for improving FedRAMP's cost-effectiveness and ensuring it remains a driving force in advancing cybersecurity for the U.S. cloud services industry. To avoid imposing burdensome reporting requirements, MITRE recommends piloting these metrics to evaluate their benefit-to-cost value.

The MITRE Cloud Engineering and Security Capability Areas, along with their enthusiastic Subject Matter Experts, are ready to provide additional support and commentary to implement these metrics, ultimately advancing the effectiveness of cloud-based national cyber defenses.