MITRE's Response to the OMB RFI on FedRAMP Penetration Testing

April 24, 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 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 (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 level to the enterprise level, integrating policy, mission, and technology considerations. The General Services Administration cites the ECAF as a best practice, and the framework has received international recognition.

In response to recent significant cyber breaches of government information technology (IT) infrastructure, many of which were orchestrated by state actors, MITRE has also established the Cloud Safe Task Force (CSTF). 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 CSTF's goal is to align industry and government efforts in developing a unified response to ensure the security of our nation's crucial digital infrastructure against relentless cyber threats. Both government and industry participated in the inaugural meeting of the task force on December 4, 2023. MITRE leveraged recommendations from and discussions with community members in this meeting, in addition to our own insights, to craft this response.

Overarching Comments

Before delving into specific comments on the draft FedRAMP Penetration Guidance, we present broader, evidence-based observations that are crucial for enhancing national cybersecurity. These insights, currently under consideration by the CSTF as part of the MITRE Cloud Safe Initiative,[1]

[1] D. Powner, et al. Cloud Safe Task Force: Recommendation Roadmap. 2024. MITRE, https://www.mitre.org/sites/default/files/2024-02/PR-24-0403-cloud-safe-task-force-recommendation-roadmap.pdf.

guide our review comments and will aid the Office of Management and Budget (OMB) in crafting a more impactful document.

Technical and Procedural Aspects of the FedRAMP Pen Testing Program

Active Vulnerability Discovery as a Pen Testing Objective. MITRE recommends a more comprehensive definition of the ultimate objective of pen testing. This should extend beyond the confines of assessment and authorization (A&A) activities to encompass the discovery of vulnerabilities and gathering of contextual information necessary for communicating actionable vulnerability information. Rather than viewing pen testing as a one-off activity for A&A, it should be considered a complementary process that enhances routine cyber operations.

Integrating Pen Testing as an Integral Part of Continuous Monitoring. Today's cyber battlespace is asymmetric, with adversaries continuously launching attack campaigns to uncover vulnerabilities. Existing continuous monitoring programs primarily focus on discovering indicators of compromise and known vulnerabilities to support cyber incident response and mitigation. As a result, adversaries often identify zero-day vulnerabilities before defenders do, creating a significant gap in our national cybersecurity defenses.

Threat Hunting as a Parallel to Penetration Testing. While pen testing focuses on identifying weaknesses at the perimeter, it is equally important to consider internal threats. This is where threat hunting comes into play. Threat hunting is a proactive approach to identifying threats that may already be present within the system, rather than waiting for an alert or incident to occur. It involves a deep understanding of the system and the potential behaviors of threats, allowing for the detection of anomalies that may indicate a compromise. We recommend that FedRAMP guidance also emphasize the importance of threat hunting as a parallel to pen testing, to ensure a comprehensive approach to system security.

Use of Adversary Emulation in Pen Testing. This approach, which can be implemented in a variety of ways and using an array of tools,[2] offers significant benefits. These benefits include a greater focus on cyber threat intelligence–driven defense, more grounded and realistic security posture and risk assessments, and the use of tools that enhance the automation and efficiency of red and purple teaming. Emulating adversarial behavior realistically enables quantifying the feedback that adversaries receive from systems under assessment. This feedback can then be analyzed to gain a better understanding of potential shifts in adversary behavior and resulting kill chain pivots.

Use of Predictive Cloud-Specific Adversary Threat Modeling for Continuous Testing. For pen testing to serve as an effective routine cybersecurity operation, it must go beyond identifying known vulnerabilities to also discover zero-day vulnerabilities. This proactive stance is vital to outpace adversaries' zero-day vulnerability discovery campaigns. Solely focusing on known vulnerabilities during pen testing is akin to driving while looking only in the rearview mirror. The integration of predictive threat modeling activities is necessary to support adversary emulation in pen testing. This requires the involvement of technology-specific subject matter experts, especially in the realm of cloud computing, who are proficient in the systems and services of the cloud service offering (CSO) under examination. We established the MITRE-

[2] Adversary Emulation and Red Teaming. 2024. MITRE ATT&CK, https://attack.mitre.org/resources/get-started/adversary-emulation-and-red-teaming/. Last accessed April 12, 2024.

CSA Cloud Adversarial Vectors, Exploits, and Threats (CAVEaT) Working Group[3] for this purpose. MITRE has also developed other predictive threat models, like ATLAS™[4] and FiGHT™[5] for AI and 5G systems, respectively. We strongly recommend continuous execution of predictive threat modeling to keep pace with evolving CSOs and their innovations to the maximum extent possible.

Use of Pen Testing Results and Disclosure of Vulnerabilities. To maximize the impact of pen testing, it is essential to use the results for immediate mitigation of discovered vulnerabilities and for disclosure programs to inform other industry participants, cloud service providers (CSPs), and potentially impacted consumers. To date, continuous monitoring reports are not made publicly available, and there are no efforts to extract greater value from the reports by sharing their content with a broader audience. We recommend that both FedRAMP continuous monitoring and pen testing results be made available to the Cybersecurity and Infrastructure Security Agency (CISA) to facilitate a broader government understanding and potential response.

Additionally, we suggest that FedRAMP consider implementing a program to provide real-time commercial cloud cyber risk information to government consumers. Such a program could feature a real-time metrics dashboard indicating the risk posture of specific government instances in commercial clouds or the risk posture of commercial clouds hosting government workloads. In today's multi-cloud industry, the ability to enact defense measures on the move is realizable. However, the indicators necessary to initiate these defensive capabilities are currently unavailable to government consumers.

Rules of Engagement for Routine and Recurrent Penetration Testing. Implementing continuous testing as prescribed here will undoubtedly be challenging. It will require industry buy-in and negotiation of the rules of engagement, a key objective of the CSTF. Success is unlikely without a collaborative partnership between industry and government. Industry will have valid concerns regarding the integrity and availability of their systems and services. If third-party assessment organizations (3PAOs) are tasked with implementing continuous testing activities and programs, CSPs will require assurances that their proprietary information will be protected. Additionally, industry will want to have input on the timing and handling of vulnerability disclosures. These and other factors will have to be considered in the development and negotiation of an effective FedRAMP Continuous Testing Program. Despite these challenges, MITRE believes that the benefits to national cybersecurity will be substantial.

Organizational and Risk Management Considerations in FedRAMP Pen Testing Program

Independent 3PAOs or Other Pen Testing Organizations. The document frequently refers to "3PAOs" performing pen testing. We suggest amending the language to "independent 3PAOs or other organizations" for the following reasons:

[3] CAVEaT™. 2024. Cloud Security Alliance, https://cloudsecurityalliance.org/research/working-groups/caveat. Last accessed April 12, 2024.

[4] MITRE ATLAS. 2024. MITRE, https://atlas.mitre.org/. Last accessed April 12, 2024.

[5] FiGHT™. 2024. MITRE, https://fight.mitre.org/. Last accessed April 12, 2024.

- 3PAOs, given their specific experience in initial accreditation of cloud services, could potentially face a perceived conflict of interest if they perform pen testing on a service they helped accredit.
- Independence can be maintained if the original accreditation 3PAO is not the same as the pen testing organization.
- Pen testing requires a different skill set than accreditation. Not all 3PAOs may specialize in pen testing skills.
- 3PAOs tend to be in high demand by CSPs and may lack the resources to perform both accreditation and pen testing services.
- Government agencies frequently contract with cybersecurity companies to perform pen testing of their own environments. This is highly commendable and helps to ensure the security of a specific agency. However, a program of government-wide independent pen testing will provide whole-of-government security, including for multiple critical infrastructures.

Pen Testing Scoping and Rules of Engagement. Pen testing should be a combination of standard testing of known methods of exploiting security loopholes and innovative adversary techniques. Given that bad actors are constantly innovating and improvising, U.S. cybersecurity defenses must recognize and strive to stay ahead. The scoping of pen testing should shift focus from mandatory testing activities to tailoring assessments based on the targeted system, its functionality, and its purpose. This approach will yield better results and will reduce the burden for all parties involved. Rather than mandating attack vectors for the penetration test, testing goals should be set based on the CSO's critical functions to ensure a more risk-focused effort based on likely adversaries and system threats. Policies and practices should allow for a tiered approach to pen testing. As an illustration of this approach, the following table outlines how testing could be based on the stages of the cyber attack life cycle[6], measuring the defender's actions to identify, respond to, and recover (e.g., incident response) from the attack:

Attack Phase	Pen Testing Defense Success Criteria
1. Recon—the adversary develops a target	1. Recognize when the defender is being targeted and successfully repel attacker
2. Weaponize—the attack is put in a form to be executed on the victim's computer/network	2. N/A
3. Deliver—this stages involves the weaponization of the identified vulnerability	3. Recognize the attempt to deliver a "weapon" and successfully deny the attack; report the incident
4. Exploit—the initial attack on the target is executed	4. Successfully recognize and deny the attack; report the incident
5. Control—mechanisms are employed to manage the initial victims	5. Recognize and prevent Command and Control communications
6. Execute—the adversary executes the plan leveraging numerous techniques	6. Identify the attack and the attackers; maintain resiliency and operations of the systems under attack; perform procedures

[6] https://www2.mitre.org/public/industry-perspective/documents/lifecycle-ex.pdf.

	to deny access by the attackers and protect the data; report the incident
7. Persistence—long-term access is achieved	7. First, detect attempts to secure a persistent presence and evade detection; second, mitigate potential threats and report the incident
8. Innovate—new and novel approaches to cyber attacks are attempted	8. Continually improve defense capabilities at the levels necessary for operations

Overall Observation on the Draft Document

Risk Management Versus Checklist Approach. The current focus of the document seems to be based on a checklist perspective rather than a risk management perspective. For example, the requirements for mandatory attack vectors in paragraph 3.1 contradict a risk management approach that tailors the pen test to the targeted system, its functionality, and its purpose. Adopting a risk management perspective would be beneficial as it allows for a more tailored and dynamic approach to security, taking into account the unique threats and vulnerabilities of each system. This approach can lead to more effective identification and mitigation of risks, enhancing the overall security posture of the system.

Section-Specific Comments

Page 1, About this Document, 2nd paragraph
Comment: We agree that testing an "organization's ability to identify and respond to security incidents" should be part of a penetration test. However, that is not described anywhere else in this document. The document does discuss notification procedures as part of the rules of engagement on pages 12 and 18, but it does not mention anything about the organization's ability to detect, respond, or recover from the incident, now how to evaluate the adequacy of these responses.

Page 4, 2.2 Attack Models, Bullet List of Enterprise and Mobile
Comment: While the approach used in listing the high-level Enterprise and Mobile ATT&CK Model Tactics is clear, and the "goal of testing to attain all of the above" is laudable, some considerations need to be made for the Mobile Matrix. Certain tactics and techniques, such as Drive-By Compromise, Lockscreen Bypass, Replication Through Removable Media, Network Effects, and Remote Service Effects, are specific to mobile devices and are unlikely to fall within the scope of the CSO authorization boundary. Responsibility for individual mobile devices typically falls on the individual user (and for government furnished equipment-only access to a CSO) it is likely under a separate mobile device system boundary. Tactics and techniques specific to the Mobile Matrix should focus on the targeted system components provided as part of the CSO to avoid confusion between the authorizing official (AO), CSP, and 3PAO.

Page 5, 3.1 Mandatory Attack Vectors
Comment: The six listed attack vectors may or may not be appliable to the CSO. Making the vectors mandatory puts a compliance focus on them as opposed to a risk management focus. Tailoring assessments based on the targeted system, its functionality, and its purpose enables a better result and reduces burden for the parties involved. Setting goals, rather than mandating

attack vectors for the penetration test based on the CSO critical functions, ensures a more risk-focused effort based on likely adversaries and system threats.

Page 6, 3.1.1 Attack Vector 1: External to Corporate, 1st paragraph
Comment: Move the last sentence to the "Email Phish Campaign" section to reduce confusion. Placing this statement at the higher level could cause confusion between the AO, CSP, and 3PAO regarding the "Non-Credentialed-Based Phishing Attack," which assesses the potential for code execution.

Page 14, Testing Schedule Requirements
Comment: Rather than waiting 12 months for another 3PAO-managed activity (i.e., compliance perspective), there should be options for more frequent threat-driven testing activities. The document includes no discussion about using automated assessment efforts such as adversary emulation as an option for more frequent or continuous penetration testing. Consider including those options.

Page 16, Rules of Engagement/Test Plan, 3rd paragraph
Comment: The bullet point "Wireless network penetration" is confusing. Do any CSOs have a wireless network component? If this means "mobile application penetration" or something similar, be more specific.

Page 19, 3PAOs Staffing Requirements
Comment: Privacy

1. Risks
    a. Inadvertent exposure of sensitive personal information
    b. Loss of data
    c. Unethical pen testers
    d. Unintended disclosures of data (mosaic effect)
2. Mitigation Strategies
    a. Encrypt sensitive personal information (i.e., Privacy-Enhancing Technologies)
    b. Vet pen testers to ensure they have proper clearances to access data
    c. Log pen testing activities
3. Outlier: European Union ENISA Certification Scheme for Cloud Providers DRAFT[7]
    a. Requires CSPs to conduct pen testing and other activities
    b. Should cloud vendors be subject to both requirements?

[7] ENISA Cybersecurity Certification of Cloud Services. 2021. European Union Agency for Cybersecurity, https://www.enisa.europa.eu/events/eventfiles/enisa-cybersecurity-certification-of-cloud-services-presentation. Last accessed April 19, 2024.