hackerone

August 21, 2025

VIA EMAIL: pete@fedramp.com

General Services Administration
1800 F Street NW, Washington D.C.

Re: RFC-0012 FedRAMP Continuous Vulnerability Management Standard

Dear Pete Waterman,

HackerOne Inc. (HackerOne) submits the following comments in response to FedRAMP's Continuous Vulnerability Management Standard.[1] We appreciate the opportunity to provide input, and we thank FedRAMP for its continued leadership in promoting public and private sector collaboration to strengthen cloud security and resilience across the federal government.

By way of background, HackerOne is a global leader in offensive security solutions. Our HackerOne Platform combines AI with the ingenuity of the largest community of security researchers to find and fix security, privacy, and AI vulnerabilities across the software development lifecycle. The platform offers bug bounty, vulnerability disclosure, pentesting, AI red teaming, and code security. We are trusted by industry leaders like Amazon, Anthropic, Crypto.com, General Motors, GitHub, Goldman Sachs, Uber, and the U.S. Department of Defense.

As agencies and cloud service providers face increasingly sophisticated and frequent cyber threats, it is critical that vulnerability management programs are not only comprehensive but also flexible and aligned with the evolving threat landscape. The draft standard represents a meaningful step in that direction, and we offer the following recommendations to further strengthen its impact:

1. Explicit Inclusion of a Vulnerability Disclosure Policy (VDP)

To address these risks and strengthen FedRAMP's continuous vulnerability management framework, we recommend aligning the standard more closely with commercial security best practices for coordinated vulnerability disclosure. While the FedRAMP program clearly states that cloud service providers should be able to meet and validate requirements using simple changes and automated capabilities, the draft is missing a commercial security best practice critical to managing vulnerabilities: the establishment of a Vulnerability Disclosure Program (VDP).

[1] FedRAMP RFC -0012, Continuous Vulnerability Management Standard, https://www.fedramp.gov/rfcs/0012/.

Recommendation: We recommend that FedRAMP include a requirement within the FRR-CVM section for all FedRAMP-authorized cloud service providers to implement and maintain publicly accessible VDPs. A proposed requirement could be inserted as FRR-CVM-01A, placed immediately before FRR-CVM-02.

Providers MUST establish and maintain programs that meet the requirements and timeframes in this standard to detect, evaluate, report, mitigate, and remediate vulnerabilities; these requirements supplement controls in FedRAMP Rev5 Baselines and Key Security Indicators in FedRAMP 20x. *Such programs MUST include a Vulnerability Disclosure Program (VDP) that provides clear reporting channels, safe harbor protections for good-faith security researchers, and processes to ensure that vulnerability information is shared responsibly and not disclosed prematurely in ways that would increase exploitation risk.*

VDPs offer a structured and effective framework for receiving, identifying, and triaging vulnerability reports. Often referred to as the internet's "see something, say something" policy, VDPs encourage individuals to report security risks they encounter, allowing organizations to address these issues promptly before they can be exploited.[2] VDPs help organizations reduce blind spots, respond to real-world threats faster, and continuously harden systems against emerging risks.

This addition would be consistent with long-standing federal policies and priorities. The Internet of Things Cybersecurity Improvement Act of 2020 mandated VDPs for information systems across civilian federal agencies.[3] That same year, the Office of Management and Budget's Memorandum M-20-32[4] and the Department of Homeland Security's Binding Operational Directive 20-01[5] reinforced this approach by requiring federal agencies to implement VDPs as part of their baseline cybersecurity practices. NIST SP 800-53 Revision 5 further supports this model, which calls for organizations to establish mechanisms for receiving and addressing vulnerability reports from external sources.[6] Building on this foundation, the Federal Contractor Cybersecurity Vulnerability Reduction Act, which was reintroduced in the House and Senate this year, proposes to extend this requirement to all U.S. government contractors.[7] In all, embedding VDPs into the baseline expectations for cloud service providers will help harmonize standards across federal systems and reduce risk to federal data and operations. Ultimately, doing so will not only strengthen the federal government's security posture but also signal a commitment to proactive vulnerability management.

---

[2] HackerOne VDP Report, https://www.hackerone.com/sites/default/files/2021-03/vulnerability-disclosure-policy-what-is-it-why-you-need-one-how-to-get-started.pdf

[3] Public Law No: 116-207, https://www.congress.gov/116/plaws/publ207/PLAW-116publ207.pdf.

[4] OMB memorandum 20-32, https://www.whitehouse.gov/wp-content/uploads/2020/09/M-20-32.pdf

[5] DHS BOD 20-01, https://www.cisa.gov/news-events/directives/bod-20-01-develop-and-publish-vulnerability-disclosure-policy

[6] National Institute of Standards and Technology (NIST), Special Publication 800-53, Security and Privacy Controls for Information Systems and Organizations, Sept. 2020, https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final.

[7] S.1899, Federal Cybersecurity Vulnerability Reduction Act, 119th Cong., https://www.congress.gov/bill/119th-congress/senate-bill/1899.

2. Avoid Premature Disclosure of Unmitigated Vulnerabilities

HackerOne recognizes FedRAMP's commitment to establishing clear and consistent expectations for cloud service providers. At the same time, RFC-0012, as currently drafted, appears to introduce a new government-wide policy on vulnerability reporting within the U.S. government. While the Federal Information Security Modernization Act (FISMA) provides a framework for managing risks to federal information systems, its statutory language does not mandate the disclosure of vulnerabilities before they are mitigated. OMB Circular A-130, which implements FISMA guidance, defines information security continuous monitoring as maintaining ongoing awareness of security risks, vulnerabilities, threats, and incidents to support risk-based decisions.[8] This underscores the importance of assessing and managing risks on a continual basis, but it does not require organizations to expose unmitigated vulnerabilities prematurely.

Mandatory early reporting of unmitigated vulnerabilities under FedRAMP could create significant security and operational risks. Disclosing vulnerabilities before they are addressed gives potential attackers actionable information, increasing the likelihood of exploitation, targeted attacks, or surveillance. Centralizing unpatched vulnerability reports, particularly in repositories accessible across federal agencies, could inadvertently concentrate risk, making federal systems and their supporting CSPs more attractive targets. Under the FedRAMP proposal, cloud service providers may also "be required to provide additional information or details about vulnerabilities, including sensitive information that would likely lead to exploitation."[9] Even if CSPs are not required to forward full technical specifications, "mere knowledge of a vulnerability's existence in a feature of some product is sufficient for a skillful person to discover it for themselves."[10] Historically, unpatched vulnerabilities have remained undisclosed precisely because early exposure increases this possibility.

HackerOne has consistently advocated[11] against requirements to disclose vulnerabilities regardless of mitigation status, as such requirements may undermine established best practices in responsible vulnerability management and weaken both domestic and global cybersecurity standards.

Recommendation: Update Sections FRR-CVM-07 and FRR-CVM-TM-01.

Providers MUST NOT share any specific sensitive information about vulnerabilities that would likely lead to exploitation at any point, but MUST share ~~sufficient~~ information about vulnerabilities for ~~oversight, tracking~~, analysis, ~~action, and risk assessment~~ with ~~all necessary~~ need -to-know parties after mitigation is complete.

[8] ,Office of Management & Budget, *Circular No. A-130: Managing Information as a Strategic Resource* (revised Nov. 28, 2000), https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf.
[9] FedRAMP RFC -0012, Continuous Vulnerability Management Standard https://www.fedramp.gov/rfcs/0012/
[10] CERT, Guide to Coordinated Vulnerability Disclosure, 5.7 Disclosure Timing, Sep. 16, 2019, https://vuls.cert.org/confluence/display/CVD/5.7+Disclosure+Timing#id-5.7DisclosureTiming-ReleasingPartialInf.
[11] How EU Lawmakers Can Make Mandatory Vulnerability Disclosure Responsible, https://www.helpnetsecurity.com/2023/08/21/vulnerability-disclosure/.

Providers ~~MUST provide up-to-date vulnerability reports to all necessary parties at least monthly and SHOULD provide these continuously.~~ MUST provide reports focused on mitigated vulnerabilities and remediation status.

* * *

HackerOne thanks FedRAMP for its continued commitment to secure, modern, and resilient cloud services and appreciate your consideration of our recommendations. We strongly encourage FedRAMP to follow existing U.S. vulnerability management best practices and ensure organizations are provided sufficient time and support to mitigate vulnerabilities before disclosure.

Respectfully Submitted,

Ilona Cohen
Chief Legal and Policy Officer
HackerOne