FedRAMP Vulnerability Detection and Response Standard

- **Release:** 25.09B
- **Published:** 2025-09-11
- **Designator:** VDR
- **Description:** This update moves the remediation table from FRR-VDR-TF-HI-07 to FRR-VDR-TF-HI-08, adds a clarification on application to Rev5, and fixes a few minor typos. No actual breaking/modifying changes were made to content.

Front Matter

Effective Date(s) & Overall Applicability

- **FedRAMP 20x**:
  - This release is effective **2025-09-15** for **20x**.
  - Phase One Pilot participants have one year from authorization to fully implement this standard but must demonstrate continuous quarterly progress.
  - Phase Two Pilot participants must demonstrate significant progress towards implementing this standard prior to authorization.
- **FedRAMP Rev5**:
  - This release is effective **2025-10-08** for **R5.VDR.B1** *(tentatively)*.
  - This release is fully optional for Rev5. Cloud service offerings who intend to adopt this standard MUST enroll in the Rev5 VDR Beta(s) and obtain approval from FedRAMP prior to halting any currently required Rev5 Continuous Monitoring process.
  - Providers should participate in the FedRAMP Rev5 Community Working Group at https://fedramp.gov/community to follow this process and request participation in the Closed Beta.
  - FedRAMP is tentatively planning for a Rev5 VDR Open Beta to begin sometime in FY26 Q2 with optional wide release possibly in FY26 Q3 or Q4.

Documentation Guidelines

The following FedRAMP documentation guidelines apply to this document:

- The capitalized key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in IETF RFC 2119.
- FedRAMP-specific terms defined in FRD-ALL (FedRAMP Definitions) are italicized throughout this document for reference.

Background & Authority

- OMB Circular A-130, Managing Information as a Strategic Resource OMB Circular A-130 defines continuous monitoring as "maintaining ongoing awareness of information security, vulnerabilities, threats, and incidents to support agency risk management decisions."
- 44 USC § 3609 (a)(7) The FedRAMP Authorization Act (44 USC § 3609 (a)(7)) directs the Administrator of the General Services Administration to "coordinate with the FedRAMP Board, the Director of the Cybersecurity and Infrastructure Security Agency, and other entities identified by the Administrator, with the concurrence of the Director and the Secretary, to establish and regularly update a framework for continuous monitoring..."

Purpose

The FedRAMP Vulnerability Detection and Response Standard ensures FedRAMP Authorized cloud service offerings use automated systems to effectively and continuously identify, analyze, prioritize, mitigate, and remediate vulnerabilities and related exposures to threats; and that information related to these activities are effectively and continuously reported to federal agencies for the purposes of ongoing authorization.

The Vulnerability Detection and Response standard defines minimum security requirements that cloud service providers must meet to be FedRAMP Authorized while allowing them flexibility in how they implement and adopt the majority of FedRAMP's requirements and recommendations. This creates a marketplace where cloud service providers can compete based on their individual approach and prioritization of security and agencies can choose to adopt cloud services with less effective security programs for less sensitive use cases while prioritizing cloud services with high performing security programs when needed.

Over time, FedRAMP will automatically review the machine-readable authorization data shared by participating cloud service providers to begin scoring cloud service offerings based on how effectively they meet or exceed the requirements and recommendations in this and other FedRAMP 20x standards.

All existing FedRAMP requirements, including control statements, standards, and other guidelines that reference vulnerability scanning or formal Plans of Action and Milestones (POA&Ms) are superseded by this standard and MAY be ignored by providers of cloud service offerings that have met the requirements to adopt this standard with approval by FedRAMP.

Expected Outcomes

- Cloud service providers following commercial security best practices will be able to meet and validate FedRAMP security requirements with simple changes and automated capabilities
- Federal agencies will be able to easily, quickly, and effectively review and consume security information about the service to make informed risk-based authorizations based on their use cases

---

Requirements

FRR-VDR

These requirements apply ALWAYS to ALL FedRAMP Authorized cloud services based on the current Effective Date(s) and Overall Applicability of this standard.

FRR-VDR-01

> Providers MUST systematically, *persistently*, and *promptly* discover and identify *vulnerabilities* within their *cloud service offering* using appropriate techniques such as assessment, scanning, threat intelligence, vulnerability disclosure mechanisms, bug bounties, supply chain monitoring, and other relevant capabilities; this process is called *vulnerability detection*.

FRR-VDR-02

> Providers MUST systematically, *persistently*, and *promptly* track, evaluate, monitor, *mitigate*, *remediate*, assess exploitation of, report, and otherwise manage all detected vulnerabilities within their *cloud service offering*; this process is called *vulnerability response*.

FRR-VDR-03

> Providers MUST follow the requirements and recommendations outlined in FRR-VDR-TF regarding timeframes for *vulnerability detection* and *response*.

> *Note: Providers are strongly encouraged to build programs that consistently exceed these thresholds. Performance will be measured by FedRAMP for comparison between providers and scoring within the FedRAMP Marketplace.*

FRR-VDR-04

> Providers MAY sample effectively identical *information resources*, especially machine-based *information resources*, when performing *vulnerability detection* UNLESS doing so would decrease the efficiency or effectiveness of *vulnerability detection*.

FRR-VDR-05

> Providers SHOULD evaluate *detected vulnerabilities*, considering the context of the *cloud service offering*, to identify logical groupings of affected *information resources* that may improve the efficiency and effectiveness of *vulnerability response* by consolidating further activity; requirements and recommendations in this standard are then applied to these consolidated groupings of *vulnerabilities* instead of each individual detected instance.

FRR-VDR-06

> Providers SHOULD evaluate *detected vulnerabilities*, considering the context of the *cloud service offering*, to determine if they are *false positive vulnerabilities*.

FRR-VDR-07

> Providers MUST evaluate *detected vulnerabilities*, considering the context of the *cloud service offering*, to determine if they are *likely exploitable vulnerabilities*.

FRR-VDR-08

> Providers MUST evaluate *detected vulnerabilities*, considering the context of the *cloud service offering*, to determine if they are *internet-reachable vulnerabilities*.

FRR-VDR-09

> Providers MUST evaluate *detected vulnerabilities*, considering the context of the *cloud service offering*, to estimate the *potential adverse impact* of exploitation on government customers AND assign one of the following *potential adverse impact* ratings:
>
> - **N1**: Exploitation could be expected to have *negligible adverse effects* on one or more *agencies* that use the *cloud service offering*.
> - **N2**: Exploitation could be expected to have *limited adverse effects* on one or more *agencies* that use the *cloud service offering*.
> - **N3**: Exploitation could be expected to have a *serious adverse effect* on one *agency* that uses the *cloud service offering*.
> - **N4**: Exploitation could be expected to have a *catastrophic adverse effect* on one *agency* that uses the *cloud service offering* OR a *serious adverse effect* on more than one federal agency that uses the *cloud service offering*.
> - **N5**: Exploitation could be expected to have a *catastrophic adverse effect* on more than one *agency* that uses the *cloud service offering*.

FRR-VDR-10

> Providers SHOULD consider at least the following factors when considering the context of the *cloud service offering* to evaluate *detected vulnerabilities*:
>
> 1. **Criticality**: How important are the systems or information that might be impacted by the *vulnerability*?
> 2. **Reachability**: How might a threat actor reach the *vulnerability* and how *likely* is that?
> 3. **Exploitability**: How easy is it for a threat actor to exploit the *vulnerability* and how *likely* is that?

4. **Detectability**: How easy is it for a threat actor to become aware of the *vulnerability* and how *likely* is that?
5. **Prevalence**: How much of the *cloud service offering* is affected by the *vulnerability*?
6. **Privilege**: How much privileged authority or access is granted or can be gained from exploiting the *vulnerability*?
7. **Proximate Vulnerabilities**: How does this *vulnerability* interact with previously *detected vulnerabilities*, especially *partially* or *fully mitigated vulnerabilities*?
8. **Known Threats**: How might already known threats leverage the *vulnerability* and how *likely* is that?

FRR-VDR-11

Providers MUST document the reason and resulting implications for their customers when choosing not to meet FedRAMP recommendations in this standard; this documentation MUST be included in the *authorization data* for the *cloud service offering*.

FRR-VDR-AY

This section provides guidance on the application of this standard, including recommendations for implementing high quality *vulnerability detection* and *response* programs; providers who follow some or all of these will be better positioned to meet future FedRAMP authorization requirements.

FRR-VDR-AY-01

If it is not possible to *fully mitigate* or *remediate detected vulnerabilities*, providers SHOULD instead *partially mitigate vulnerabilities promptly*, progressively, and *persistently*.

FRR-VDR-AY-02

Providers SHOULD make design and architecture decisions for their *cloud service offering* that mitigate the risk of *vulnerabilities* by default AND decrease the risk and complexity of *vulnerability detection* and *response*.

FRR-VDR-AY-03

Providers SHOULD use automated services to improve and streamline *vulnerability detection* and *response*.

FRR-VDR-AY-04

Providers SHOULD automatically perform *vulnerability detection* on representative samples of new or *significantly changed information resources*.

FRR-VDR-AY-05

Providers SHOULD NOT weaken the security of *information resources* to facilitate vulnerability scanning or assessment activities.

FRR-VDR-AY-06

Providers SHOULD NOT deploy or otherwise activate new machine-based *information resources* with *Known Exploited Vulnerabilities*.

FRR-VDR-RP

This section identifies FedRAMP-specific reporting requirements and recommendations for *vulnerabilities*.

FRR-VDR-RP-01

> Providers MUST report *vulnerability detection* and *response* activity to all necessary parties *persistently*, summarizing ALL activity since the previous report; these reports are *authorization data* and are subject to the FedRAMP Authorization Data Sharing (ADS) standard.

FRR-VDR-RP-02

> Providers SHOULD include high-level overviews of ALL *vulnerability detection* and *response* activities conducted during this period for the *cloud service offering;* this includes vulnerability disclosure programs, bug bounty programs, penetration testing, assessments, etc.

FRR-VDR-RP-03

> Providers MUST NOT irresponsibly disclose specific sensitive information about *vulnerabilities* that would *likely* lead to exploitation, but MUST disclose sufficient information for informed risk-based decision-making to all necessary parties.
>
> *Note: See FRR-VDR-EX for exceptions to this requirement.*

FRR-VDR-RP-04

> Providers MAY responsibly disclose *vulnerabilities* publicly or with other parties if the provider determines doing so will NOT *likely* lead to exploitation.

FRR-VDR-RP-05

> Providers MUST include the following information (if applicable) on *detected vulnerabilities* when reporting on *vulnerability detection* and *response* activity, UNLESS it is an *accepted vulnerability*:
>
> 1. Provider's internally assigned tracking identifier
> 2. Time and source of the detection
> 3. Time of completed evaluation
> 4. Is it an *internet-reachable vulnerability* or not?
> 5. Is it a *likely exploitable vulnerability* or not?
> 6. Historically and currently estimated *potential adverse impact* of exploitation
> 7. Time and level of each completed and evaluated reduction in *potential adverse impact*
> 8. Estimated time and target level of next reduction in *potential adverse impact*
> 9. Is it currently or is it likely to become an *overdue vulnerability* or not? If so, explain.
> 10. Any supplementary information the provider responsibly determines will help federal agencies assess or mitigate the risk to their *federal information* within the *cloud service offering* resulting from the *vulnerability*
> 11. Final disposition of the *vulnerability*

FRR-VDR-RP-06

> Providers MUST include the following information on *accepted vulnerabilities* when reporting on *vulnerability detection* and *response* activity:
>
> 1. Provider's internally assigned tracking identifier
> 2. Time and source of the detection
> 3. Time of completed evaluation
> 4. Is it an *internet-reachable vulnerability* or not?
> 5. Is it a *likely exploitable vulnerability* or not?
> 6. Currently estimated *potential adverse impact* of exploitation
> 7. Explanation of why this is an *accepted vulnerability*

8. Any supplementary information the provider determines will responsibly help federal agencies assess or mitigate the risk to their *federal information* within the *cloud service offering* resulting from the *accepted vulnerability*

FRR-VDR-EX

These exceptions MAY override some or all of the FedRAMP requirements and recommendations in this standard.

FRR-VDR-EX-01

Providers MAY be required to share additional *vulnerability* information, alternative reports, or to report at an alternative frequency as a condition of a FedRAMP Corrective Action Plan or other agreements with federal agencies.

FRR-VDR-EX-02

Providers MAY be required to provide additional information or details about *vulnerabilities*, including sensitive information that would *likely* lead to exploitation, as part of review, response or investigation by necessary parties.

FRR-VDR-EX-03

Providers MUST NOT use this standard to reject requests for additional information from necessary parties which also include law enforcement, Congress, and Inspectors General.

FRR-VDR-TF

This section provides guidance on timeframes that apply to all impact levels of FedRAMP authorization for activities required or recommended in this standard; these timeframes are thresholds that secure providers should consistently strive to exceed by significant margins.

FRR-VDR-TF-01

Providers MUST report *vulnerability detection* and *response* activity to all necessary parties in a consistent format that is human readable at least monthly.

FRR-VDR-TF-02

Providers SHOULD *remediate Known Exploited Vulnerabilities* according to the due dates in the CISA Known Exploited Vulnerabilities Catalog (even if the vulnerability has been *fully mitigated*) as required by CISA Binding Operational Directive (BOD) 22-01 or any successor guidance from CISA.

FRR-VDR-TF-03

Providers MUST categorize any vulnerability that is not or will not be *fully mitigated* or *remediated* within 192 days of evaluation as an *accepted vulnerability*.

FRR-VDR-TF-LO

This section provides guidance on timeframes that apply specifically to FedRAMP Low authorizations for activities required or recommended in this standard; these timeframes are thresholds that secure providers should consistently strive to exceed by significant margins.

FRR-VDR-TF-LO-01

> Providers SHOULD make all recent historical *vulnerability detection* and *response* activity available in a *machine-readable* format for automated retrieval by all necessary parties (e.g. using an API service or similar); this information SHOULD be updated *persistently*, at least once every month.

FRR-VDR-TF-LO-02

> Providers SHOULD *persistently* perform *vulnerability detection* on representative samples of similar machine-based *information resources*, at least once every week.

FRR-VDR-TF-LO-03

> Providers SHOULD *persistently* perform *vulnerability detection* on all *information resources* that are *likely* to *drift*, at least once every month.

FRR-VDR-TF-LO-04

> Providers SHOULD *persistently* perform *vulnerability detection* on all *information resources* that are NOT *likely* to *drift*, at least once every six months.

FRR-VDR-TF-LO-05

> Providers SHOULD evaluate ALL *vulnerabilities* as required by FRR-VDR-07, FRR-VDR-08, and FRR-VDR-09 within 7 days of *detection*.

FRR-VDR-TF-LO-06

> Providers SHOULD *partially mitigate, fully mitigate,* or *remediate vulnerabilities* to a lower *potential adverse impact* within the timeframes from evaluation shown below (in days), factoring for the current *potential adverse impact*, *internet reachability,* and *likely exploitability*:

Potential Adverse Impact	LEV + IRV	LEV + NIRV	NLEV
N5	4	8	32
N4	8	32	64
N3	32	64	192
N2	96	160	192

FRR-VDR-TF-LO-07

> Providers SHOULD *mitigate* or *remediate* remaining *vulnerabilities* during routine operations as determined necessary by the provider.

FRR-VDR-TF-MO

This section provides guidance on timeframes that apply specifically to FedRAMP Moderate authorizations for activities required or recommended in this standard; these timeframes are thresholds that secure providers should consistently strive to exceed by significant margins.

FRR-VDR-TF-MO-01

> Providers SHOULD make all recent historical *vulnerability detection* and *response* activity available in a *machine-readable* format for automated retrieval by all necessary parties (e.g. using an API service or similar); this information SHOULD be updated *persistently*, at least once every 14 days.

FRR-VDR-TF-MO-02

> Providers SHOULD *persistently* perform *vulnerability detection* on representative samples of similar machine-based *information resources*, at least once every 3 days.

FRR-VDR-TF-MO-03

> Providers SHOULD *persistently* perform *vulnerability detection* on all *information resources* that are *likely* to *drift*, at least once every 14 days.

FRR-VDR-TF-MO-04

> Providers SHOULD *persistently* perform *vulnerability detection* on all *information resources* that are NOT *likely* to *drift*, at least once per month.

FRR-VDR-TF-MO-05

> Providers SHOULD evaluate ALL *vulnerabilities* as required by FRR-VDR-07, FRR-VDR-08, and FRR-VDR-09 within 5 days of *detection*.

FRR-VDR-TF-MO-06

> Providers SHOULD treat *internet-reachable likely exploitable vulnerabilities* with a *potential adverse impact* of N4 or N5 as a security incident until they are *partially mitigated* to N3 or below.

FRR-VDR-TF-MO-07

> Providers SHOULD *partially mitigate, fully mitigate,* or *remediate vulnerabilities* to a lower *potential adverse impact* within the timeframes from evaluation shown below, factoring for the current *potential adverse impact*, *internet reachability,* and *likely exploitability*:

Potential Adverse Impact	LEV + IRV	LEV + NIRV	NLEV
N5	2	4	16
N4	4	8	64
N3	16	32	128
N2	48	128	192

FRR-VDR-TF-MO-08

> Providers SHOULD *mitigate* or *remediate* remaining *vulnerabilities* during routine operations as determined necessary by the provider.

FRR-VDR-TF-HI

This section provides guidance on timeframes that apply specifically to FedRAMP High authorizations for activities required or recommended in this standard; these timeframes are thresholds that secure providers should consistently strive to exceed by significant margins.

FRR-VDR-TF-HI-01

> Providers SHOULD make all recent historical *vulnerability detection* and *response* activity available in a *machine-readable* format for automated retrieval by all necessary parties (e.g. using an API service or similar); this information SHOULD be updated *persistently*, at least once every 7 days.

FRR-VDR-TF-HI-02

> Providers SHOULD *persistently* perform *vulnerability detection* on representative samples of similar machine-based *information resources*, at least once per day.

FRR-VDR-TF-HI-03

> Providers SHOULD *persistently* perform *vulnerability detection* on all *information resources* that are *likely* to *drift*, at least once every 7 days.

FRR-VDR-TF-HI-04

> Providers SHOULD *persistently* perform *vulnerability detection* on all *information resources* that are NOT *likely* to *drift*, at least once every month.

FRR-VDR-TF-HI-05

> Providers SHOULD evaluate ALL *vulnerabilities* as required by FRR-VDR-07, FRR-VDR-08, and FRR-VDR-09 within 2 days of *detection*.

FRR-VDR-TF-HI-06

> Providers SHOULD treat *internet-reachable likely exploitable vulnerabilities* with a *potential adverse impact* of N4 or N5 as a security incident until they are *partially mitigated* to N3 or below.

FRR-VDR-TF-HI-07

> Providers SHOULD treat *likely exploitable vulnerabilities* that are NOT *internet-reachable* with a *potential adverse impact* of N5 as a security incident until they are partially mitigated to N4 or below.

FRR-VDR-TF-HI-08

> Providers SHOULD *partially mitigate vulnerabilities* to a lower *potential adverse impact* within the maximum time-frames from evaluation shown below, factoring for the current *potential adverse impact*, *internet reachability,* and *likely exploitability*:

Potential Adverse Impact	LEV + IRV	LEV + NIRV	NLEV
N5	.5	1	8
N4	2	8	32
N3	8	16	64

Potential Adverse Impact	LEV + IRV	LEV + NIRV	NLEV
N2	24	96	192

FRR-VDR-TF-HI-09

> Providers SHOULD *mitigate* or *remediate* remaining *vulnerabilities* during routine operations as determined necessary by the provider.

FRR-VDR-AG

The section provides guidance for agencies that apply under 44 USC § 3613 (e) which states that the assessment and materials within a FedRAMP authorization package "shall be presumed adequate for use in an agency authorization to operate cloud computing products and services."

FRR-VDR-AG-01

> Agencies SHOULD review the information provided in vulnerability reports at appropriate and reasonable intervals commensurate with the expectations and risk posture indicated by their Authorization to Operate, and SHOULD use automated processing and filtering of machine readable information from cloud service providers.
>
> *Note: FedRAMP recommends that agencies only review overdue and _accepted vulnerabilities* with a *potential adverse impact* of N3 or higher unless the cloud service provider recommends mitigations or the service is included in a higher risk federal information system. Furthermore, *accepted vulnerabilities* generally only need to be reviewed when they are added or during an updated risk assessment due to changes in the agency's use or authorization._

FRR-VDR-AG-02

> Agencies SHOULD use *vulnerability* information reported by the Provider to maintain Plans of Action & Milestones for agency security programs when relevant according to agency security policies (such as if the agency takes action to mitigate the risk of exploitation or authorized the continued use of a cloud service with *accepted vulnerabilities* that put agency information systems at risk).

FRR-VDR-AG-03

> Agencies SHOULD NOT request additional information from cloud service providers that is not required by this FedRAMP standard UNLESS the head of the agency or an authorized delegate makes a determination that there is a demonstrable need for such.
>
> *Note: This is related to the Presumption of Adequacy directed by 44 USC § 3613 (e).*

FRR-VDR-AG-04

> Agencies MUST inform FedRAMP after requesting any additional *vulnerability* information or materials from a cloud service provider beyond those required by this policy by sending a notification to info@fedramp.gov.
>
> *Note: This is an OMB policy; agencies are required to notify FedRAMP in OMB Memorandum M-24-15 section IV (a).*

Technical assistance

FRA-VDR

Purpose: This Technical Assistance provides additional context behind the intent and goals of certain aspects of this standard that have caused significant confusion or requests for clarification during public comment. This assistance is initially designed for 20x Phase Two/Three and the Rev5 Closed Beta Balance Improvement Test.

Disclaimer: Every cloud service provider is different, every architecture is different, and every environment is different. Best practices and technical assistance MUST NOT be used as a checklist. All examples are for discussion purposes ONLY.

FRA-VDR-01

FedRAMP focuses on internet-reachable (rather than internet-accessible) to ensure that any service that might receive a payload from the internet is prioritized if that service has a vulnerability that can be triggered by processing the data in the payload. The simplest way to prevent exploitation of internet-reachable vulnerabilities is to intercept, inspect, filter, sanitize, reject, or otherwise deflect triggering payloads before they are processed by the vulnerable resource; once this prevention is in place the vulnerability should no longer be considered an internet-reachable vulnerability.

A classic example of an internet-reachable vulnerability on systems that are not typically internet-accessible is SQL injection (https://en.wikipedia.org/wiki/SQL_injection), where an application stack behind a load balancer and firewall with no ability to route traffic to or from the internet can receive a payload indirectly from the internet that triggers the manipulation or compromise of data in a database that can only be accessed by an authorized connection from the application server on a private network.

Another simple example is the infamous Log4Shell (https://en.wikipedia.org/wiki/Log4Shell) vulnerability from 2021, where exploitation was possible via vulnerable internet-reachable resources deep in the application stack that were often not internet-accessible themselves.

FRA-VDR-02

The simple reality is that most traditional vulnerabilities discovered by scanners or during assessment are not likely to be exploitable; exploitation typically requires an unrealistic set of circumstances that will not occur during normal operation. The likelihood of exploitation will vary depending on so many factors that FedRAMP will not recommend a specific framework for approaching this beyond the recommendations and requirements in this document.

The proof, ultimately, is in the pudding - providers who regularly evaluate vulnerabilities as not likely exploitable without careful consideration are more likely to suffer from an adverse impact where the root cause was an exploited vulnerability that was improperly evaluated. If done recklessly or deliberately, such actions will have a potential adverse impact on a provider's FedRAMP authorization.
