FedRAMP Significant Change Notification Requirements

- **Release:** 25.06B
- **Published:** 2025-08-24
- **Designator:** SCN
- **Description:** Minor non-breaking updates to align term definitions and highlighted terms across updated materials (definitions are now in FRD-ALL).

Front Matter

Effective Date(s) & Overall Applicability

- **FedRAMP 20x**:
  - This release is effective **2025-06-17** for **20xP1**.
  - These requirements apply to all participants in the FedRAMP 20x Phase One pilot.
  - Key Security Indicators for Configuration Management (KSI-CMT) should be updated in alignment with the Significant Change Notification Standard.
- **FedRAMP Rev5**:
  - This release is effective **2025-07-07** for **R5.SCN.B1** *(tentatively)*.
  - These requirements will be initially tested and evaluated for Rev5 in the SCN Closed Beta (B1).
  - Providers MUST participate in a Balance Improvement Test to transition from the Significant Change Request process to the new Significant Change Notification process prior to wide release of this process for Rev5. Providers should participate in the FedRAMP Rev5 Community Working Group at https://www.fedramp.gov/community/ to follow this process.

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

- 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 [OMB] Director and the [DHS] Secretary, to establish and regularly update a framework for continuous monitoring..."
- OMB Memorandum M-24-15 on Modernizing FedRAMP section VI states "FedRAMP should seek input from CSPs and develop processes that enable CSPs to maintain an agile deployment lifecycle that does not require advance Government approval, while giving the Government the visibility and information it needs to maintain ongoing confidence in the FedRAMP-authorized system and to respond timely and appropriately to incidents."

Purpose

The Significant Change Notification (SCN) standard establishes conditions for FedRAMP authorized cloud service providers to make most significant changes without requiring advance government approval. Agency authorizing officials

who authorize the use of FedRAMP authorized cloud services are expected to account for the risk of cloud service providers making changes to improve the service.

This standard broadly identifies four types of significant changes, from least impactful to most impactful:

1. Routine Recurring
2. Adaptive
3. Transformative
4. Impact Categorization

These categories, and the resulting requirements, apply only to significant changes.

Expected Outcomes

- Cloud service providers will securely deliver new features and capabilities for government customers at the same speed and pace of delivery for commercial customers, without needing advance government approval
- Federal agencies will have equal access to features and capabilities as commercial customers without sacrificing the visibility and information they need to maintain ongoing confidence in the service

---

Requirements

FRR-SCN

These requirements apply ALWAYS to ALL *significant changes* based on current Effective Date(s) and Overall Applicability

FRR-SCN-01

> Providers MUST notify all necessary parties when Significant Change Notifications are required, including at least FedRAMP and all agency customers. Providers MAY share Significant Change Notifications publicly or with other parties.

FRR-SCN-02

> Providers MUST follow the procedures documented in their security plan to plan, evaluate, test, perform, assess, and document changes.

FRR-SCN-03

> Providers MUST evaluate and type label all *significant changes*, then follow FedRAMP requirements for the type.

FRR-SCN-04

> Providers MUST maintain auditable records of these activities and make them available to all necessary parties.

FRR-SCN-05

> Providers MUST keep historical Significant Change Notifications available to all necessary parties at least until the service completes its next annual assessment.

FRR-SCN-06

> All parties SHOULD follow FedRAMP's best practices and technical assistance on *significant change* assessment and notification where applicable.

FRR-SCN-07

> Providers MAY notify necessary parties in a variety of ways as long as the mechanism for notification is clearly documented and easily accessible.

FRR-SCN-08

> Providers MUST make ALL Significant Change Notifications and related audit records available in similar human-readable and compatible *machine-readable* formats.

FRR-SCN-09

> Providers MUST include at least the following information in Significant Change Notifications:
>
> 1. Service Offering FedRAMP ID
> 2. 3PAO Name (if applicable)
> 3. Related POA&M (if applicable)
> 4. Significant Change type and explanation of categorization
> 5. Short description of change
> 6. Reason for change
> 7. Summary of customer impact, including changes to services and customer configuration responsibilities
> 8. Plan and timeline for the change, including for the verification, assessment, and/or validation of impacted Key Security Indicators or controls
> 9. Copy of the business or security impact analysis
> 10. Name and title of approver

FRR-SCN-10

> Providers MAY include additional relevant information in Significant Change Notifications.

FRR-SCN-EX

These exceptions MAY override some or all of the FedRAMP requirements for this standard.

FRR-SCN-EX-01

> Providers MAY be required to delay *significant changes* beyond the standard Significant Change Notification period and/or submit *significant changes* for approval in advance as a condition of a formal FedRAMP Corrective Action Plan or other agreement.

FRR-SCN-EX-02

> Providers MAY execute *significant changes* (including *transformative* changes) during an emergency or incident without meeting Significant Change Notification requirements in advance ONLY if absolutely necessary. In such emergencies, providers MUST follow all relevant procedures, notify all necessary parties, retroactively provide all Significant Change Notification materials, and complete appropriate assessment after the incident.

FRR-SCN-RR

These requirements apply ONLY to *significant changes* of type *routine recurring*.

FRR-SCN-RR-01

> Providers SHOULD NOT make formal Significant Change Notifications for *routine recurring* changes; this type of change is exempted from the notification requirements of this standard.

FRR-SCN-AD

These requirements apply ONLY to *significant changes* of type *adaptive*.

FRR-SCN-AD-01

> Providers MUST notify all necessary parties within ten business days after finishing *adaptive* changes, also including the following information:
>
> 1. Summary of any new risks identified and/or POA&Ms resulting from the change (if applicable)

FRR-SCN-TF

These requirements apply ONLY to *significant changes* of type *transformative*.

FRR-SCN-TF-01

> Providers SHOULD engage a third-party assessor to review the scope and impact of the planned change before starting *transformative* changes if human validation is necessary. This review SHOULD be limited to security decisions that require human validation. Providers MUST document this decision and justification.

FRR-SCN-TF-02

> Providers MUST notify all necessary parties of initial plans for *transformative* changes at least 30 business days before starting *transformative* changes.

FRR-SCN-TF-03

> Providers MUST notify all necessary parties of final plans for *transformative* changes at least 10 business days before starting *transformative* changes.

FRR-SCN-TF-04

> Providers MUST notify all necessary parties within 5 business days after finishing *transformative* changes, also including the following information:
>
> 1. Updates to all previously sent information

FRR-SCN-TF-05

> Providers MUST notify all necessary parties within 5 business days after completing the verification, assessment, and/or validation of *transformative* changes, also including the following information:
>
> 1. Updates to all previously sent information

> 2. Summary of any new risks identified and/or POA&Ms resulting from the change (if applicable)
> 3. Copy of the security assessment report (if applicable)

FRR-SCN-TF-06

> Providers MUST publish updated service documentation and other materials to reflect *transformative* changes within 30 business days after finishing *transformative* changes.

FRR-SCN-TF-07

> Providers MUST allow agency customers to OPT OUT of *transformative* changes whenever feasible.

FRR-SCN-IM

These requirements apply ONLY to *significant changes* of type *impact categorization*.

FRR-SCN-IM-01

> Providers MUST follow the legacy Significant Change Request process or full re-authorization for *impact categorization* changes, with advance approval from an identified lead agency, until further notice.

Technical assistance

FRA-SCN

Purpose: This Technical Assistance helps stakeholders evaluate and label *significant changes* by type as required by *FRR-SCN-03*. This assistance is designed for the 20x Phase One Pilot and Rev5 Closed Beta Balance Improvement Test. The Significant Change Notification Requirements will be tested, evaluated, and improved in partnership with stakeholders based on real-world experience.

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-SCN-03

Once a change has been identified as a *significant change* in general, FedRAMP recommends next determining if a change is of the type *routine recurring*. If it is not, work down from the highest impact to lowest to identify the type of change.

1. Is it a *significant change*?
2. If it is, is it a *routine recurring* change?
3. If it is not, is it an *impact categorization* change?
4. If it is not, is it a *transformative* change?
5. If it is not, then it is an *adaptive* change.

FRA-SCN-RR

Activities that match the *routine recurring significant change* type are performed *regularly* and routinely by cloud service providers to address flaws or vulnerabilities, address incidents, and generally perform the typical maintenance and service delivery changes expected during day-to-day operations.

These changes leverage mature processes and capabilities to identify, mitigate, and remediate risks as part of the change. They are often entirely automated and may occur without human intervention, even though they have an impact on security of the service.

If the activity does not occur *regularly* and routinely then it cannot be a *significant change* of this type (e.g., replacing all physical firewalls to remediate a vulnerability is obviously not regular or routine).

Ongoing operations

Key Tests:

- Routine care and feeding by staff during normal duties
- No major impact to service availability
- Does not require executive approval

Examples:

- Provisioning or deprovisioning capacity to support service elasticity
- Changing or tuning performance configurations for instances or services
- Updating and maintaining operational handling of information flows and protection across physical and logical networks (e.g., updating firewall rules)
- Generating or refreshing API or access tokens

Vulnerability Management

Key Tests:

- Minor, incremental patching or updates
- Significant refactoring or migration process NOT required
- No breaking changes

Examples:

- Updating security service or endpoint signatures
- Routine patching of devices, operating systems, software or libraries
- Updating and deploying code that applies normal fixes and improvements as part of a regular development cycle
- Vulnerability remediation activity that simply replaces a known-bad component(s) with a better version of the exact same thing, running in the exact same way with no changes to processes

---

FRA-SCN-TF

Activities that match the *transformative significant change* type are rare for a cloud service offering, adjusted for the size, scale, and complexity of the service. Small cloud service offerings may go years without *transformative* changes, while hyperscale providers may release multiple *transformative* changes per year.

Transformative changes

Key Tests:

- Alters the service risk profile or require new or significantly different actions to address customer responsibilities
- Requires significant new design, development and testing with discrete associated project planning, budget, marketing, etc.
- Requires extensive updates to security assessments, documentation, and how a large number of security requirements are met and validated

Examples:

- The addition, removal, or replacement of a critical third party service that handles a significant portion of information (e.g., IaaS change)
- Increasing the security categorization of a service within the offering that actively handles federal information (does NOT include impact change of entire offering - see impact categorization change)
- Replacement of underlying management planes or paradigm shift in workload orchestration (e.g., bare-metal servers or virtual machines to containers, migration to kubernetes)
- Datacenter migration where large amounts of federal information is moved across boundaries different from normal day-to-day operations
- Adding a new AI-based capability that impacts federal information in a different way than existing services or capabilities (such as integrating a new third-party service or training on federal information)

FRA-SCN-AD

Activities that match the *adaptive significant change* type are a frequent and normal part of iteratively improving a service by deploying new functionality or modifying existing functionality in a way that is typically transparent to customers and does not introduce significant new security risks.

In general, most changes that do not happen *regularly* will be *adaptive* changes. This change type deliberately covers a wide range of activities in a way that requires assessment and consideration.

Service adjustments

Key Tests:

- Requires minimal changes to security plans or procedures
- Requires some careful planning and project management to implement, but does not rise to the level of planning required for transformative changes
- Requires verification of existing functionality and secure configuration after implementation

Examples:

- Updates to operating systems, containers, virtual machines, software or libraries with known breaking changes, complex steps, or service disruption
- Deploying larger than normal incremental feature improvements in code or libraries that are the work of multiple weeks of development efforts but are not considered a major new service
- Changing cryptographic modules where the new module meets the same standards and characteristics of the former
- Replacing a like-for-like component where some security plan or procedure adjustments are required (e.g., scanning tool or managed database swap)
- Adding models to existing approved AI services without exposing federal information to new services

---