

Response to FedRAMP RFC-0033

20x Phase 4 Development Tracks for 20x Class D

Submitted by: Jewel Darlington, Chief AI Governance Officer & Founder

Organization: Solutions by Jewel, Global AI Governance Advisory Firm

Contact: governance@solutionsbyjewel.com

Date: October 7, 2026

Summary

Solutions by Jewel (SBJ) offers targeted feedback on RFC-0033, consistent with FedRAMP's stated preference for explicit, targeted comments. RFC-0033 describes 20x Class D as intended for federal workloads where threats to the confidentiality, integrity, or availability of federal customer data may lead to catastrophic harm, including loss of life.

SBJ offers five recommendations, each mapped to a specific RFC-0033 proposal and each built on an existing Consolidated Rules for 2026 mechanism. A closing section addresses agency authorization authority.

1. **Anticipated requirement 1 (six-month Class C history).** Define assurance-state events that require a recorded determination of whether operating-history evidence remains representative.
2. **Anticipated requirement 2 (Class D IaaS/PaaS).** Make inherited assurance explicitly bounded and machine-identifiable in the Security Decision Record.
3. **Anticipated requirement 3 (Certified third-party information resources).** Link each material third-party information resource to its function, impact, relied-upon assurance, evidence, mitigation, and reassessment condition.
4. **SDR-CSX-KMT and anticipated requirement 4 (GRC integration).** Add evidence-level provenance, applicability, and validity fields to the Class D Security Decision Record.
5. **Hosting definitions and Track 2.** Require an explicit assurance determination when a hosting-classification change affects the certification basis.

1. Operating History and Assurance-State Continuity

RFC-0033 proposal. Anticipated Class D requirement 1 would require a service offering to hold a 20x Class C Certification with zero corrective actions for six months before becoming eligible for Class D Certification after the Phase 4 pilot.

Recommendation. SBJ supports operating history as an assurance input. SBJ recommends that the detailed Class D requirements define assurance-state events that require the provider to determine, and record in the Security Decision Record, whether evidence from the observation period remains representative of the offering seeking Class D. Candidate events include:

1. a Transformative Change affecting the architecture or certification basis;
2. migration to a materially different hosting environment;
3. addition, removal, or replacement of a third-party information resource within the Minimum Assessment Scope;

4. a material change to inherited security capabilities;
5. a material change to the mechanisms producing Key Security Indicator measures;
6. a material change in control responsibility; and
7. a FedRAMP Reportable Incident that alters the evidentiary basis for certification.

For each event type, the requirements should specify the evidence needed to evaluate its effect, whether review is full or scoped, and how the determination is recorded. A scoped determination can resolve a trigger within the existing six-month period.

Basis. CCM-OCR-AVL requires an Ongoing Certification Report every three months that summarizes, where applicable, Transformative Changes and FedRAMP Reportable Incidents, so a six-month window spans two reporting cycles. The Significant Change Notification rules supply the event inputs: their Transformative Change examples include adding, removing, or replacing a critical third-party service, replacing underlying management planes, and datacenter migration. SCN-CSO-INF already requires a plan for verifying, assessing, or validating impacted Key Security Indicators. The note to SCN-TRF-UPD scopes the post-change documentation update to service documentation such as user guides and marketplace information. For Class D, SBJ recommends extending that update to the Security Decision Record: after the SCN-TRF-NAV notification, the provider records whether prior assurance conclusions remain applicable.

SBJ professional technical position. SBJ AI Governance Architecture V1.0 states: "Derived Authorization is newly scoped authority issued as the result of an event, state or condition, decision, validation, remediation, or authorized transition." Applied to Class D eligibility, an assurance-state event calls for a newly scoped determination of what the operating-history evidence still supports. This application is SBJ's professional technical position.

2. Bounded Inheritance from Class D IaaS/PaaS

RFC-0033 proposal. Anticipated Class D requirement 2 would require cloud-hosted or hybrid-hosted Class D services to be deployed on a Class D Certified IaaS/PaaS.

Recommendation. For each FedRAMP rule or Key Security Indicator that relies on inherited assurance, the dependent provider's Security Decision Record should identify:

1. the upstream offering from which assurance is inherited;
2. the specific rule, Key Security Indicator, or capability inherited;
3. the resources and operating environment to which the inheritance applies;
4. responsibilities that remain with the dependent provider;
5. the evidence supporting the inherited assurance;
6. the dependence of that assurance on the upstream certification remaining in force; and
7. the conditions under which the inheritance must be reassessed.

These entries should be machine-identifiable in the Security Decision Record JSON schema, so that a downstream provider can determine whether a material upstream change affects its own assurance state.

Basis. SDR-CSO-FRR already requires, for each applicable rule, an explanation of implementation, verification, validation, independent verification, and independent validation. A per-rule inheritance reference is a bounded extension of that structure.

SBJ professional technical position. SBJ AI Governance Architecture V1.0 states: "An Authority Envelope is the bounded set of conditions within which an AI system or agent is authorized to act. Depending on context, the envelope may include the actor or system, action, target, tool, credential, environment, time, delegated authority, approval, stop conditions, and evidence requirements." V1.0 also states: "Derived Authorization is newly scoped authority issued as the result of an event, state or condition, decision, validation, remediation, or authorized transition." Applied to Class D infrastructure inheritance, inherited assurance is newly scoped to the dependent offering and carries the boundary of the upstream certification, covering the capabilities and conditions that certification evaluated. This application is SBJ's professional technical position.

3. Third-Party Resource Dependency Traceability

RFC-0033 proposal. Anticipated Class D requirement 3 would require third-party information resources within a Class D service's Minimum Assessment Scope to hold Class B, C, or D Certification.

Recommendation. SBJ recommends that each material third-party information resource be associated with a structured dependency record that identifies:

1. the function the resource performs;
2. the federal customer data or security property it could affect;
3. the capability or authority it holds relative to the cloud service offering;
4. the assurance relied upon, including its certification Class;
5. the evidence establishing that assurance;
6. the compensating controls limiting dependency risk; and
7. the change in the resource that would require reassessment.

SBJ also asks FedRAMP to clarify, in the October 14 requirements RFC, how a Class D provider should justify reliance on a Class B or Class C Certified resource for a function whose compromise could produce Class D-level impact.

Basis. MAS-CSO-TPR requires providers to document, for each applicable third-party information resource, its general usage and configuration, the explanation or justification for use, mitigation measures, and compensating controls. The recommended record adds the relied-upon assurance, its evidence, and the reassessment condition, linking those existing fields to the proposed Class D certification requirement.

4. Evidence Provenance, Applicability, and Validity

RFC-0033 proposal. Anticipated Class D requirement 4 would expect providers to support integration of assurance data into agency GRC systems. SDR-CSX-KMT states that Class D providers must significantly supersede lower-Class historical-metric requirements, with specifics to be set during the Phase 4 pilot.

Recommendation. SBJ recommends that Phase 4 define minimum evidence-level fields for material Class D assurance evidence, where applicable:

1. evidence source;
2. collection or observation time;
3. resource and environment to which the evidence applies;

4. applicable FedRAMP rule or Key Security Indicator;
5. method of generation;
6. verification status;
7. validation status;
8. independent verification and validation status;
9. related dependency or inherited-assurance entry;
10. period or conditions of validity; and
11. the event or condition requiring regeneration or review.

Basis. SDR-CSO-MTD requires version, date and time of last update, and source of update at the record level. SDR-CSX-KSI requires summaries of measures, persistent cycles, verification, automation verification, and validation for each Key Security Indicator. The recommended fields carry equivalent information down to individual evidence items, which is the level at which agency GRC systems ingest and evaluate assurance data. SDR-CSO-FRR already separates provider verification and validation from independent verification and validation; the recommended fields preserve that separation for automated evidence.

5. Hosting-Classification Changes

RFC-0033 proposal. RFC-0033 proposes formal definitions for cloud-hosted, self-hosted, and hybrid-hosted cloud service offerings, and Track 2 will develop self-hosted and hybrid-hosted rules for the Consolidated Rules for 2027.

Recommendation. When a cloud service offering's classification under these definitions changes, or responsibility for physical infrastructure shifts materially, the provider should record a determination covering:

1. changed responsibilities;
2. changed dependencies;
3. changed inherited assurance;
4. affected information flows;
5. affected evidence;
6. any required independent reassessment; and
7. resulting Security Decision Record updates.

Scoped review should be available where evidence supports continued applicability of existing conclusions. Several such transitions already qualify as Transformative Changes under the Significant Change Notification rules, including datacenter migration and replacement of underlying management planes. SBJ recommends routing the determination through the SCN-TRF-NAV notification, the Ongoing Certification Report, the Minimum Assessment Scope, and the Security Decision Record, and that Track 2 consider it when drafting self-hosted and hybrid-hosted rules.

SBJ professional technical position. SBJ AI Governance Architecture V1.0 states: "Transition Authorization governs whether and under what approved conditions a system may cross a governed environment, lifecycle, privilege, capability, autonomy, or consequence boundary." Its application to FedRAMP hosting classifications is SBJ's professional technical position.

6. Agency Authorization Authority

The Collaborative Continuous Monitoring rules describe shared, current authorization information supporting each agency's Information Security Continuous Monitoring strategy, with each agency making its own risk-based decisions about ongoing authorization. SBJ recommends that Class D preserve that separation between evidence generation and decision authority as material changes, evidence validity, and reassessment conditions become more explicit and machine-usable.

Scope Note

The constructs referenced in sections 1, 2, and 5 are documented in SBJ AI Governance Architecture V1.0, a governance architecture for AI systems. Their application to FedRAMP 20x Class D cloud service offerings, a broader category that includes AI systems, is SBJ's professional technical position, offered for FedRAMP's consideration during Phase 4.

V1.0 serves as the cross-cutting architecture across SBJ's methodology stack, which includes STRATA™ (GRC foundation), SIGNAL™ (AI-specific control and audit methodology), and SYNTHESIZE™ (Physical AI governance methodology).

This comment addresses the five areas above, which fall within SBJ's governance-architecture lane.

References

FedRAMP. RFC-0033, 20x Phase 4 Development Tracks for 20x Class D. <https://www.fedramp.gov/rfcs/0033/>

FedRAMP. Consolidated Rules for 2026, Security Decision Record (SDR-CSO-FRR, SDR-CSO-MTD, SDR-CSX-KSI, SDR-CSX-KMT). <https://www.fedramp.gov/2026/providers/20x/rules/security-decision-record/>

FedRAMP. Consolidated Rules for 2026, Minimum Assessment Scope (MAS-CSO-IIR, MAS-CSO-TPR). <https://fedramp.gov/2026/providers/20x/rules/minimum-assessment-scope/>

FedRAMP. Consolidated Rules for 2026, Collaborative Continuous Monitoring (CCM-OCR-AVL). <https://www.fedramp.gov/2026/providers/20x/rules/collaborative-continuous-monitoring/>

FedRAMP. Consolidated Rules for 2026, Significant Change Notification (SCN-CSO-INF, SCN-TRF-NAV, SCN-TRF-UPD). <https://fedramp.gov/2026/providers/20x/rules/significant-change-notification/>

Solutions by Jewel. SBJ AI Governance Architecture V1.0.
<https://github.com/solutionsbyjewel/sbj-ai-governance-architecture-v1>

Jewel Darlington

Chief AI Governance Officer & Founder

Solutions by Jewel, Global AI Governance Advisory Firm

governance@solutionsbyjewel.com