GovRAMP

November 2026

Request for Comments (RFC) GR – 2601

Proposed 20x Delta Assessment

Purpose of GovRAMP RFC 2601 – 20x Delta Assessment 1
Introduction 2
Proposal Overview 3
Long-Term Objective 3
This RFC seeks community feedback on: 4
The Proposed 20x Delta Assessment 4
Scope of the Proposal 4
Methodology 4
Analysis Takeaways 5
Instructions for Reviewing the Analysis: 5
Proposed Delta Assessment 7
Response Instructions 10
Submission Requirements 11
Requested Comments: 12
Response Deadline 14
Appendix: Rationale for Proposed Approach 14
Key Objectives of the proposed 20x Delta Assessment 15
Benefits of Proposed Delta Assessment 15
For Service Provider Community Serving All Levels of Government 15
For Government Users 15
Flexibility Supports Risk-Based Approach 15
Why Align with NIST 16
NIST alignment provides several important benefits: 16

Purpose of GovRAMP RFC 2601 – 20x Delta Assessment

GovRAMP is seeking stakeholder feedback on a proposed 20x Delta Assessment approach intended to support alignment between FedRAMP 20x and the GovRAMP security verification requirements. The proposed approach seeks to reduce duplicative assessment effort while maintaining the security assurance, consistency, and risk-based validation that government agencies rely on when evaluating cloud products and services.

This Request for Comments (RFC) invites government agencies, cloud service providers, third party assessment organizations (3PAOs), consultants, and other interested stakeholders to review the proposed assessment criteria and provide feedback on their clarity, effectiveness, implementation considerations, and potential impact. Feedback will inform GovRAMP's continued evaluation of the proposed approach. Participation in this RFC is open to GovRAMP members and non-members.

Comment Period

- RFC Open Date: November 2, 2026
- RFC Close Date: December 4, 2026
- Submission Method: Online (preferred) or email to rfc@govramp.org.

Attachment: GR 20x Delta Analysis Record

- The workbook contains information on the methodology, analysis and proposed approach.

Introduction

GovRAMP recognizes that maintaining multiple compliance frameworks can be challenging and resource-intensive for providers. Harmonization therefore remains a strategic priority. As such, GovRAMP formed a Framework Harmonization Working Group in April 2025 to devote focused stakeholder attention to this initiative. As regulatory requirements and the cybersecurity landscape continue to evolve, GovRAMP will continue to adapt its program to meet the needs of both government agencies and industry participants.

This RFC is in response to the publication of FedRAMP's Consolidated Rules 2026 and ongoing discussions around how to harmonize requirements for FedRAMP 20x and GovRAMP verified statuses. (References: 2026 - FedRAMP Consolidated Rules for 2026 and Security Program | GovRAMP). View more background and rationale on the approach in the Appendix.

Proposal Overview

Framework Harmonization Working Group and GovRAMP committee discussions informed the development of the proposed 20x Delta Assessment. The Delta Assessment is intended to serve as a bridge between the modernized assessment concepts being introduced

through FedRAMP 20x and the established NIST-based requirements that underpin GovRAMP and many of the security frameworks relied upon by state, local, tribal, and territorial (SLTT) governments. These include requirements and programs founded on NIST standards, such as FISMA, CJIS Security Policy, IRS Publication 1075, and CMMC.

The proposed approach aligns with key principles of FedRAMP 20x, including automation, continuous assurance, evidence reuse, and risk-based validation. At the same time, it provides additional NIST-aligned assessment objectives intended to establish a common baseline of trust and assurance for government customers. The Delta Assessment may be applied alongside a FedRAMP 20x assessment, ideally during the initial review process or subsequently, to address areas where additional testing is needed to support a GovRAMP verified status.

The goal of the Delta Assessment is to synthesize and modernize how assurance is demonstrated by emphasizing continuous visibility into risk, ongoing monitoring, and independent validation of meaningful changes to a provider's security posture. GovRAMP believes this approach can build trust while creating a more efficient, scalable, and sustainable pathway for both providers and government stakeholders.

Long-Term Objective

The overarching objective of the 20x Delta Assessment is to create a practical and sustainable path for cloud service providers serving both federal and SLTT government customers. The approach is intended to complement the FedRAMP 20x vision while maintaining the consistency and confidence government agencies require when evaluating cybersecurity risk.

GovRAMP leadership remains committed to engaging the community throughout this process and welcomes feedback to help ensure the program balances security, operational practicality, and trust across the public sector ecosystem.

This RFC seeks community feedback on:

- Whether the proposed Delta Assessment appropriately balances security assurance, operational efficiency, and the evolving needs of the GovRAMP community, including both public and private participants.
- The extent to which the proposed Delta Assessment appropriately aligns with modern authorization approaches, security validation methods, and the regulatory requirements that underpin many state and local government compliance obligations.
- Whether the Delta Assessment criteria are appropriate, clear, risk-based, implementable, and sufficient for trust decisions.
- Specific policy considerations related to System Security Plan (SSP) documentation requirements; annual penetration testing requirements; and supplemental evidence requirements related to malicious code protection.

The Proposed 20x Delta Assessment

Scope of the Proposal

The 20x Delta Assessment proposal is focused exclusively on annual assessment requirements associated with GovRAMP-verified status. This proposal does not modify GovRAMP continuous monitoring requirements and does not address FedRAMP's recently introduced Vulnerability Disclosure Reporting (VDR) and Vulnerability Exploitation Reporting (VER) requirements.

This exclusion is intentional. In August 2026, the GovRAMP Standards & Technical Committee and the GovRAMP Board directed the GovRAMP PMO to recognize FedRAMP's VDR and VER requirements as satisfying the corresponding GovRAMP continuous monitoring requirements for GovRAMP Authorized products. As a result, this proposal is limited to annual assessment activities and does not impact existing continuous monitoring.

Methodology

A standardized approach for scoping Key Security Indicators (KSIs) is needed to enable consistent and repeatable assessments across organizations.

GovRAMP selected NIST SP 800-53 Revision 5 as the basis for scoping the Delta Assessment because NIST remains the common cybersecurity foundation underlying many federal, state, local, tribal, and territorial government security programs and regulations. (Reference: Appendix).

An analysis was conducted to identify the potential NIST control coverage between FedRAMP 20x certification requirements for Class B and Class C and the requirements for GovRAMP Core, Ready and Authorized. The analysis leveraged several available machine-readable data sets, including:

1. FedRAMP's 2026 Consolidated Rules .json file available at https://raw.githubusercontent.com/fedramp/rules/refs/heads/main/fedramp-consolidated-rules.json
2. GovRAMP's Low and Moderate controls baseline published at https://govramp.org/hubfs/RFC/GR%20Controls%20Selection%20for%20All%20Baselines.xlsx
3. NIST SP800-53 and NIST SP800-53A in OSCAL format available at https://raw.githubusercontent.com/usnistgov/oscal-content/refs/heads/main/nist.gov/SP800-53/rev5/json/NIST_SP-800-53_rev5_catalog.json
4. GSA FedRAMP PMO's *Threat-Based Controls Scoring* study located at https://github.com/GSA/threat-analysis/raw/refs/heads/main/REV5-MITRE%20ATTACK%20Threat%20Analysis%20(01-07-2022).xlsx

Analysis Takeaways

As a starting point, the analysis focused on the Moderate impact level, as it is the most commonly used impact level within the GovRAMP security program. Depending on stakeholder feedback, GovRAMP may apply the same methodology to additional impact levels in a future phase of this effort.

When comparing FedRAMP 20x potential NIST control coverage to GovRAMP-verified statuses, the analysis showed:

- FedRAMP 20x has potential to meet 88.3% of GovRAMP Core NIST Control Coverage (Moderate Impact Level)
- FedRAMP 20x has potential to meet 78.8% of GovRAMP Ready NIST Control Coverage (Moderate Impact Level)
- FedRAMP 20x has potential to meet 62.4% of GovRAMP Authorized NIST Control Coverage (Moderate Impact Level).

Subsequent discussions in committee work sessions centered on the methodology for validating NIST controls. A mapped KSI may relate to a NIST control, but that alone does not prove that a provider's evidence satisfies the control or GovRAMP's assessment objectives. This resulted in a recommendation to develop a GovRAMP 20x Delta Assessment using NIST Assessment Objective language to inform the required inputs and evidence for mapped KSIs.

Instructions for Reviewing the Analysis:

View the analysis and proposal workbook at GR 20x Delta Analysis Record.

Tab 1 (*FR 20x NIST Mapping*)

- Represents the import of the 20x KSIs from the FedRAMP Consolidated Rules .json file.
- Each KSI is represented in the tab, along with its Theme Name, KSI Statement, and Related NIST SP800-53 controls as identified by FedRAMP.

Tab 2 (*20x KSIs to NIST by Rows*)

- Duplicates the data from the first tab and creates a new row for each related NIST control.
- For each control, additional information is added:
    - NIST SP800-53r5 Control Statement,
    - Indicator for selection at the GovRAMP Core, Moderate Ready, or GovRAMP Authorized baselines,
    - Any GovRAMP Parameter or guidance information,
    - NIST SP800-53A *Assessment Objective* for the control,
    - the NIST SP800-53A *Potential Assessment Methods and Objects* for the control,

and
    - The *Protection Value* assigned from the *Threat-Based Controls Scoring* study.

Tab 3 (*20x - GovRAMP – NIST Crosswalk)*

- This worksheet shows where potential alignment between 20x and GovRAMP may exist leveraging NIST 800-53 Rev.5.
- Imports NIST SP800-53 and SP800-53A OSCAL files to create a table of the currently active Rev 5 controls, Control Description, NIST Discussion, Related SP800-53 Controls, SP800-53A Assessment Objectives and Potential Assessment Methods and Objects.
- This tab is further enhanced by importing the *Risk Protection Value* assigned from the *Threat-Based Controls Scoring* study and adding indicators for selection at the GovRAMP Core, Ready (Moderate), and/or GovRAMP Authorized (Moderate) baselines, any GovRAMP Parameter or guidance information.
- The 20x KSI ID field was added to show if an 800-53 Rev. 5 control is mentioned within the 20x KSIs and, when applicable, to identify the corresponding KSI(s).
- Finally, the NIST to KSI Objective leverages the NIST Assessment Objective language to inform the GovRAMP recommendation for what inputs to include in the mapped KSI.

Tabs 4a – 6b (Crosswalk Variances for GovRAMP Core, Ready and Authorized)

- Tabs 4a – 6b are grouped into three (3) sections and represent the analysis for 20x and GovRAMP Core, 20 x and GovRAMP Ready, and 20x and GovRAMP Authorized at the Moderate Impact level.
- GovRAMP Core and 20x:
    - *Tab 4a (Missing 20x NIST – GR Core)* shows the NIST controls that GovRAMP Core covers and 20x does not (based on NIST control mappings found in the FedRAMP .json file).
    - *Tab 4b (Surplus 20x NIST – GR Core)* shows the NIST controls that 20x potentially covers that are not required for GovRAMP Core.
    - *Tab 4c (Sample Core GR KSI)* shows the proposed GovRAMP Core Delta Assessment criteria for existing KSIs (Part A) and proposed Delta Assessment criteria for those controls not found within 20x (Part B).
- GovRAMP Ready and 20x:
    - *Tab 5a (Missing 20x NIST – GR Ready)* shows the NIST controls that GovRAMP Ready covers and 20x does not (based on NIST control mappings found in the FedRAMP .json file).
    - *Tab 5b (Surplus 20x NIST – GR Ready)* shows the NIST controls that are potentially covered in 20x that are not required for GovRAMP Ready.
    - *Tab 5c (Sample Ready GR KSI)* shows the proposed GovRAMP Ready Delta Assessment criteria for existing KSIs (Part A) and proposed Delta Assessment criteria for those controls not found within 20x (Part B)

- GovRAMP Authorized and 20x:
  - *Tab 6a (Missing 20x NIST – GR Auth)* shows the NIST controls that GovRAMP Authorized covers and 20x does not (based on NIST control mappings found in the FedRAMP .json file).
  - *Tab 6b (Surplus 20x NIST – GR Auth)* shows the NIST controls that 20x potentially covers that are not required for GovRAMP Authorized.

Proposed Delta Assessment

The proposed 20x Delta Assessment is based on the crosswalk analysis of FedRAMP KSI's to NIST to GovRAMP, and includes two components:

Part A: Aligns the FedRAMP 20x KSIs and NIST guidance based on FedRAMP's .json file mapping.

Part B: Makes recommendations on approach to the missing NIST control requirements from FedRAMP's .json file mapping.

Part A – Aligns 20x KSIs and NIST Guidance (FedRAMP .json Mapping)

The table below illustrates how each 20x KSI has been defined, leveraging NIST guidance and assessment objectives.

Providers will have the option to select their Delta Assessment based on their desired GovRAMP verified status (GovRAMP Core, Ready or Authorized). For example, the higher the GovRAMP verified status, the more defined KSI guidance and assessment objectives.

View Part A proposal in Tabs 4c and 5c of the *GR20x Delta Analysis Record*.

20x KSI ID	GR KSI Guidance	GR Assessment Objectives
KSI-CNA-EIS	Indicate if..... CA-02(01) - independent assessors or assessment teams are employed to conduct control assessments. Indicate if..... CA-07(01) - independent assessors or assessment teams are employed to monitor the controls in the system on an ongoing basis.	Determine if..... CA-02(01) - independent assessors or assessment teams are employed to conduct control assessments. Determine if..... CA-07(01) - independent assessors or assessment teams are employed to monitor the controls in the system on an ongoing basis.

KSI-CNA-IBP	Indicate if..... AC-17(03) - remote accesses are routed through authorized and managed network access control points. Indicate if..... CM-02a.[01] - a current baseline configuration of the system is developed and documented; CM-02a.[02] - a current baseline configuration of the system is maintained under configuration control; CM-02b.01 - the baseline configuration of the system is reviewed and updated [the frequency of baseline configuration review and update is defined;]; CM-02b.02 - the baseline configuration of the system is reviewed and updated when required due to [the circumstances requiring baseline configuration review and update are defined;]; CM-02b.03 - the baseline configuration of the system is reviewed and updated when system components are installed or upgraded. Indicate if..... PL-10 - a control baseline for the system is selected.	Determine if..... AC-17(03) - remote accesses are routed through authorized and managed network access control points. Determine if..... CM-02a.[01] - a current baseline configuration of the system is developed and documented; CM-02a.[02] - a current baseline configuration of the system is maintained under configuration control; CM-02b.01 - the baseline configuration of the system is reviewed and updated [the frequency of baseline configuration review and update is defined;]; CM-02b.02 - the baseline configuration of the system is reviewed and updated when required due to [the circumstances requiring baseline configuration review and update are defined;]; CM-02b.03 - the baseline configuration of the system is reviewed and updated when system components are installed or upgraded. Determine if..... PL-10 - a control baseline for the system is selected.

Part B – Outstanding NIST Controls for GovRAMP Baselines (FedRAMP .json Mapping)

Some NIST controls were not mapped to FedRAMP 20x KSIs in the FedRAMP .json file and are therefore absent in the proposed GovRAMP 20x Delta Assessment (Part A). These outstanding NIST controls can be viewed in the ***GR20x Delta Analysis Record*** on Tabs 4a, 5a and 6a and show the following:

- 7 missing 20x NIST controls for GovRAMP Core (Moderate impact level)
- 17 missing 20x NIST controls for GovRAMP Ready (Moderate impact level)
- 120 missing 20x NIST controls for GovRAMP Authorized (Moderate impact level)

GovRAMP proposes the following approach to these outstanding controls and invites your feedback.

1. Evaluate the missing controls based on their MITRE Control Protection Value.
   - The GSA FedRAMP PMO's *Threat-Based Controls Scoring* study recommended a cut score of 41.772 for control selection.
   - If the value is less than 41.772, do not include the control in a Delta Assessment.
   - If the value is greater than or equal to 41.772, include the control.

GovRAMP Verified Status (Moderate Impact Level)	# of Controls Not Mapped to a KSI	# of Controls > or = 41.772	# of Controls < 41.772
Core	*7*	4	3
Ready	*17*	4	3
Authorized	*120*	24	96

Reference: [GitHub - GSA/threat-analysis · GitHub]

2. Using NIST-related controls information, combine related outstanding controls into groups (aka a new KSI) and leverage the NIST Assessment Guidance for creating and evaluating the new KSI.
   - View an example of this methodology in ***GR20x Delta Analysis Record*** applied for GovRAMP Core in *Tab 4c-Sample Core GR KSI* and applied for GovRAMP Ready in *Tab 5c – Sample Ready GR KSI*.

Should this approach be affirmed in the RFC process, staff will complete the analysis for all verified statuses and impact levels.

Response Instructions

GovRAMP welcomes feedback from all stakeholders, including government agencies, cloud service providers, assessors, consultants, and industry partners. Responses will be summarized and reported in aggregate. Individual respondents and organizations will not be identified or attributed. To ensure balanced representation of stakeholder perspectives, feedback will be categorized and analyzed by stakeholder group (e.g., government agencies, cloud service providers, and 3PAOs/consultants).

Submission Requirements

Responses may be submitted online via a form (preferred method) or emailed to rfc@govramp.org.

Emailed responses must include the following:

- Subject line: **"RFC for 20x Delta Assessment"**
- Following information:
    - Organization or government entity name
    - Primary point of contact
    - Email address
    - Phone number
    - GovRAMP Member: Yes or No
    - What type of entity best describes you?
        - Government Entity (Federal, State, Local, K-12, Higher Education, Tribal Territory or Other)
        - Private Sector:
            - Service Provider
            - 3PAO
            - Consultant
        - Other (please explain)
    - If Service Provider:
        - Do you have a Rev 5 assessment?
        - Do you have a 20x Certification?
        - Are you planning for a 20x Certification?

Requested Comments:

To facilitate review of all comments received, please provide your comments utilizing the following format/template. Responses are optional for each question.

1. **Overall Approach**
   How well does the proposed Delta Assessment approach balance security assurance, operational efficiency, and the evolving needs of the GovRAMP community?

2. **Alignment with Government Security Requirements**
   Please provide your comments. For example, does the proposed Delta Assessment appropriately align with:
   - Modern authorization approaches and emerging assessment models;
   - Security validation and assurance objectives; and
   - Common federal requirements and regulatory frameworks that impact state, local, tribal, and territorial governments (e.g., FISMA, CJIS, IRS, CMS, SSA, etc. and related requirements)?

3. **Delta Assessment Criteria – Part A**
   Please provide feedback on the proposed Delta Assessment (Part A) criteria, such as:
   - Whether the criteria provide sufficient security assurance;
   - Whether the criteria appropriately focus on meaningful security risk;
   - Whether the criteria help government agencies make informed compliance decisions
   - Any criteria that should be added, modified, or removed.

4. **Delta Assessment Criteria – Part B**
   Please provide feedback on the proposed approach (Part B) to outstanding NIST controls, such as:
   - Pros and cons of this approach;
   - Any criteria that should be added, modified or removed; or
   - Alternative approaches to the outstanding controls.

5. **System Security Plan (SSP) Requirement**
   FedRAMP 20x does not require a traditional System Security Plan (SSP) as part of its assessment approach. However, NIST SP 800-53 control PL-2 (System Security Plan) is a requirement for GovRAMP Authorized status.
   - Should GovRAMP continue to require an SSP for GovRAMP Authorized status when evaluating providers assessed under FedRAMP 20x?
   - Should SSP requirements differ by GovRAMP status level (Core, Ready, and Authorized)?
   - Are there alternative forms of documentation that could satisfy PL-2 requirements while reducing administrative burden? For example, should GovRAMP accept OSCAL-formatted components, as satisfying substantive objectives of PL-2?
   - What impact would maintaining, modifying, or removing the SSP requirement have on provider adoption, assessor consistency, and government trust?

6. **Annual Penetration Testing Requirement (CA-8)**
   FedRAMP 20x does not require annual penetration testing. GovRAMP Authorized status currently requires annual penetration testing to satisfy CA-8 requirements.

- Should GovRAMP continue to require annual penetration testing for GovRAMP Authorized status?
- If annual penetration testing remains a requirement, should GovRAMP permit:
    - Independent third-party penetration testing; or
    - Internally conducted penetration testing that meets established testing standards?
- If internally conducted penetration testing is permitted, GovRAMP recommends adherence to *GovRAMP Penetration Testing Guidance*. How might organizations demonstrate that their internal testing processes and results meet the intent and requirements of the guidance? For example, should a 3PAO review internally conducted penetration tests for adequacy and alignment with GovRAMP Penetration Testing Guidance?
- Are there alternative approaches that could provide equivalent assurance to annual penetration testing?

7. **Supplemental Evidence for SI-3 (Malicious Code Protection)**
   FedRAMP 20x does not explicitly require supplemental evidence related to SI-3 (Malicious Code Protection). GovRAMP currently requires evidence supporting malicious code protection capabilities for GovRAMP Core, Ready, and Authorized statuses.
    - Should SI-3 evidence be included as a required component of the Delta Assessment for all GovRAMP verified status, including Core, Ready and Authorized?
    - Are there alternative methods of validating malicious code protection that would provide a comparable level of assurance with less administrative burden?
        - For example, what types of modern cloud-native evidence (e.g., container image vulnerability scanning, CI/CD static/dynamic analysis, eBPF runtime threat detection) adequately satisfy SI-3 without requiring legacy endpoint anti-virus screenshots?

8. **Impact**
   How would adoption of the proposed Delta Assessment affect your organization? (Please explain your response)
    - Significantly Positive
    - Somewhat Positive
    - No Significant Impact
    - Somewhat Negative
    - Significantly Negative

9. **Additional Comments**
   Please provide any additional comments, concerns, recommendations, or implementation considerations related to the proposed Delta Assessment.

Based on stakeholder input, GovRAMP will publish guidance for providers who have already completed a 20x certification and for those planning to pursue a 20x certification who also wish to achieve or maintain a GovRAMP verified status.

Response Deadline

Responses must be received **no later than 5:00 p.m. Eastern Time on Friday, December 4, 2026.**

GovRAMP appreciates your time and thoughtful feedback as we evaluate how best to harmonize with emerging federal approaches while maintaining the trust, consistency, and security assurance that participating governments and providers rely upon.

Appendix: Rationale for Proposed Approach

Key Objectives of the proposed 20x Delta Assessment

- Allow service providers the flexibility to apply the 20x Delta Assessment for their selected GovRAMP verified status of GovRAMP Core, Ready, or Authorized environment.
- Streamline unnecessary assessment burden and streamline maintenance to maintain both a GovRAMP verified status and a FedRAMP 20x certification.
- Establish a standardized approach for scoping 20x Key Security Indicators (KSIs) to enable consistent and repeatable assessments across organizations. To achieve this objective, the proposed Delta Assessment leverages NIST's published assessment guidance.
- Support risk-based annual assessment decisions that complement GovRAMP's existing continuous monitoring requirements.

Benefits of Proposed Delta Assessment

For Service Provider Community Serving All Levels of Government

- **Verify once, serve many**
    - The Delta Assessment enables providers to achieve certification while demonstrating NIST compliance important to many agencies.

- **Clear guidance for Key Security Indicator (KSI) scoping related to 20x**
    - Eliminates guesswork around agency needs and requirements, providing clear scoping guidance for assessment and setting consistent expectations for all stakeholders.

For Government Users

- **Trust and assurance in reliability of a consistent standard**
    - With common scoping, government users can have confidence in a common baseline for security.

- **Continuous assurance**
    - The combination of FedRAMP 20x automation and GovRAMP's centralized Program Management Office (PMO) shared services gives government users ongoing visibility into security risks, real-time status updates, and timely notifications of elevated risk conditions, enabling more informed and proactive risk management.

Flexibility Supports Risk-Based Approach

GovRAMP's risk-based approach recognizes that security requirements must align with the sensitivity of the data being protected. Allowing providers to map to the GovRAMP verified status that best fits their services and customer needs, whether it's GovRAMP Core, GovRAMP Ready, or GovRAMP Authorized, promotes flexibility while maintaining appropriate security assurance.

In practice, GovRAMP Core is commonly suited for commercial, public, or internal business data; GovRAMP Ready is often appropriate for sensitive or confidential information; and GovRAMP Authorized (at low, moderate or high impact level) is intended for highly regulated data types such as FTI, CJI, SSA, CMS data and other regulated government information.

Why Align with NIST

GovRAMP's proposal to align the 20x Delta Assessment with NIST-based requirements reflects the reality that NIST remains the foundational cybersecurity framework upon which most government security programs are built. While FedRAMP 20x introduces important innovations in how security assurance is demonstrated, state, local, tribal, and territorial (SLTT) governments, as well as many regulatory and procurement programs, continue to rely on NIST standards as the common framework for evaluating cybersecurity risk.

Reference: The following regulations are based on or built on NIST guidance and affect public agencies and providers.

- Federal Information Security Modernization Act FISMA
- NIST publication FIPS 200, which defines minimum security requirements for Federal Information and Information Systems
- U.S. Veterans Affairs Agency July 2026 Memo
- IRS Publication 1075 (Rev. 12-2026)
- FBI CJIS Security Policy Resource Center — LE
- SSA Security Information | Data Exchange | SSA Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration, Technical System Security Requirements (TSSR)
- CMS Medicaid Enterprise Systems (MES) certification process - SMC Guidance.pdf

NIST alignment provides several important benefits:

Consistency Across Government and Regulatory Programs
NIST security baselines underpin many federal and state cybersecurity requirements, creating a common framework for security expectations across jurisdictions. State agencies are routinely audited against these requirements. Maintaining a NIST-based foundation aligns GovRAMP with the regulatory environment in which SLTT governments operate.

Simultaneously, NIST provides a well-known, trusted basis for assessing the cloud service providers that support regulated and federally funded programs.

For state governments required to comply with NIST-based federal regulatory requirements, the inability to demonstrate compliance can have consequences beyond an audit finding. Depending on the applicable federal program and the nature of the deficiency, potential consequences may include:

- Federal funding impacts, including funding restrictions, delayed funding, or additional grant conditions.
- Increased federal oversight, including high-risk designations, additional reporting requirements, corrective action plans, and increased administrative burden.
- Increased state or local oversight, including legislative scrutiny, additional reporting obligations, administrative burden, and associated costs.
- Restrictions on federal information sharing, including suspension or termination of access to federal data, potentially disrupting mission-critical government services and causing reputational harm.

A Common Baseline for Government and Vendors
GovRAMP is designed to provide a centralized verification model that government agencies can rely upon when making risk-based decisions. Because participating governments use GovRAMP assessments as a shared source of security assurance, a common and well-understood baseline is essential. NIST SP 800-53 Rev. 5 provides that baseline by establishing standardized security requirements that support consistent assessments, comparable results, and trusted risk decisions across jurisdictions. This allows providers to demonstrate security once and serve many government customers while giving agencies confidence in a common level of assurance.

Support for Framework Harmonization
By maintaining a NIST-aligned foundation while embracing the modernization principles of FedRAMP 20x, GovRAMP can reduce duplication and improve interoperability between federal and SLTT cybersecurity requirements. This approach enables providers to leverage work performed for one program to support compliance efforts across multiple government markets, reducing administrative burden while preserving trust, assurance, responsibility, and accountability.

GovRAMP views NIST alignment as a complementary approach to FedRAMP 20x that helps translate emerging federal modernization efforts into a framework that remains broadly useful and trusted across the public-sector ecosystem.

The goal is to enable innovation in security assessment while maintaining consistency, transparency, and assurance that government stakeholders expect.

Reference: View October 9th Framework Harmonization Working Group for more background

Community engagement remains central to this effort, and GovRAMP welcomes feedback as it works to advance a security program that is practical, risk-informed, and trusted across the public sector ecosystem.