GovRAMP

Version 1.0

2026 GOVRAMP SYMPOSIUM

A Path Forward for Framework Harmonization

Recommendations on how to move from analysis to action for regulatory and framework harmonization.

March 9, 2026

Ronald Reagan Building · Washington, D.C.
Held in coordination with the Billington State & Local CyberSecurity Summit

Executive Summary

The United States faces a systemic challenge in aligning cybersecurity requirements across federal, state, and sector-specific frameworks. While these frameworks address legitimate and often mission-specific risks, the lack of coordination among them has produced significant duplication, increased cost, and unnecessary complexity for government and industry alike.

The impacts of this fragmentation are well-documented. Multiple U.S. Government Accountability Office (GAO) reviews over several years have quantified both the prevalence and cost of conflicting requirements. Recommendations have been issued, pilot efforts have been initiated, and interagency coordination mechanisms have been established — yet meaningful, sustained progress has remained limited.

Recent federal initiatives reflect growing recognition that the current model is unsustainable. FedRAMP modernization efforts, NIST Rev. 5 balance improvements, and the evolution of programs such as CMMC signal movement toward automation, standardized evidence, and greater reuse of assessments. However, when pursued as discrete initiatives — absent an overarching harmonization strategy — these efforts cannot fully address the underlying structural problem.

The challenge is not a lack of technical solutions. It is the absence of a coherent policy framework that enables those solutions to operate across programs.

This white paper outlines the key policy actions identified by federal, state, and local security leaders, procurement officials, and service providers at the GovRAMP 2026 Symposium to move from analysis to execution. Participants expressed broad consensus that the ecosystem is ready for operational harmonization — and that meaningful progress can be achieved under existing authority.

In particular, the Symposium surfaced strong agreement that the Office of Management and Budget (OMB), in coordination with the Office of the National Cyber Director (ONCD), is uniquely positioned to lead this work. Formal guidance establishing shared baselines, expanded recognition of equivalent controls, and phased reciprocity across frameworks represents the highest-impact near-term action available.

GovRAMP does not seek to replace federal standards or to position its program as the controlling framework. Instead, GovRAMP offers a practical, operational model for how reciprocity, shared baselines, and evidence reuse can function across federal, state, and local environments — and stands ready to support federal leadership as a technical partner and convener.

KEY FINDINGS AND RECOMMENDATIONS AT A GLANCE

Harmonization efforts span multiple administrations.
Both the Trump and Biden administrations initiated actions to address regulatory fragmentation. Foundational analysis and coordination mechanisms already exist, providing a strong basis for continued execution.

The objective is not a single framework.
The goal is a "do once, use many" model in which security evidence produced under one rigorous framework satisfies equivalent requirements across others.

OMB guidance is the highest-impact near-term lever.
Formal reciprocity guidance issued under existing authority can enable immediate progress, provided it is paired with agency coordination and clear parameters for implementation.

GovRAMP's role is operational and convening.
GovRAMP contributes tested reciprocity models, crosswalk tools, and stakeholder coordination capacity in support of federally led harmonization efforts.

Section 1: The Challenge — Fragmentation and Its Costs

Cybersecurity requirements across federal and state programs have developed independently over time. While each framework addresses legitimate mission needs, they operate largely in parallel rather than in alignment. The cumulative effect of this fragmentation is substantial — and growing.

The issue is not the existence of cybersecurity frameworks. It is the lack of coordination among them, which results in overlapping but inconsistent requirements for organizations operating across jurisdictions.

UNDERSTANDING THE CONTROL PARAMETER PROBLEM

Most major federal cybersecurity frameworks — including FBI's Criminal Justice Information Services (CJIS) security policy, IRS Publication 1075, Centers for Medicare & Medicaid Services (CMS) information security requirements, and Social Security Administration (SSA) information security requirements — are built on a shared foundation: NIST SP 800-53. In principle, this should enable interoperability.

In practice, divergence occurs at the point of customization.

NIST SP 800-53 intentionally requires agencies to define specific control parameters based on mission context: thresholds for account lockout, audit log retention periods, scan frequencies, and similar requirements. These parameters translate abstract controls into auditable obligations.

Because agencies have defined these parameters independently, state and local governments subject to multiple federal programs are often required to meet conflicting specifications for controls that are substantively identical in purpose.

Recent experience also demonstrates that alignment across frameworks is achievable. Symposium participants pointed to ongoing work related to the FBI's Criminal Justice Information Services (CJIS) Security Policy as an example of how legacy requirements can be incrementally modernized and better aligned with NIST SP 800-53 without reducing security rigor, including through practical crosswalks and overlays developed to clarify control implementation (see GovRAMP's CJIS overlay).

While CJIS remains a distinct program with unique statutory and operational requirements, efforts to clarify requirements, align controls to NIST-based foundations, and modernize interpretive guidance have helped reduce friction for practitioners navigating overlapping federal obligations. This progress illustrates a broader point raised throughout the Symposium: harmonization does not require replacing existing frameworks, but rather establishing clearer baselines and shared interpretations so security work performed once can be more broadly recognized.

GAO's 2020 analysis illustrates this problem clearly. For the same core controls, agencies imposed materially different parameter values — forcing states to adopt multiple configurations, maintain separate documentation sets, and undergo redundant assessments.

The security objective remains the same. The administrative burden multiplies.

A formally established common baseline addresses this issue directly. Rather than each agency tailoring SP 800-53 in isolation, a shared baseline would define common parameters recognized across participating frameworks. Agencies would retain the ability to apply justified program-specific overlays, but foundational controls would be assessed once, with evidence reused across programs.

This is the operational core of the "do once, use many" model.

THE STATE AND LOCAL BURDEN

State governments operate at the intersection of multiple federal cybersecurity regimes simultaneously. A single state may administer Medicaid programs under CMS rules, operate law enforcement systems governed by CJIS, manage tax systems under IRS Publication 1075, and administer benefits programs subject to SSA requirements — each assessed independently, often using different terminology and evidence formats.

The burden this creates is uneven. Larger states may sustain dedicated compliance teams to manage complexity. Smaller states, counties, and municipalities — often with only one or two IT staff — face the same requirements with a fraction of the capacity.

For these jurisdictions, the compliance overhead can become a barrier to achieving the security outcomes the frameworks are intended to support.

The burden is compounded at the federal level as well. Agencies independently assess the same state systems without audit reciprocity, duplicating effort and cost across government.

The consistent ask from state and local practitioners is not to reduce standards. It is to align them — so that rigorous security work performed once is recognized across programs.

FRAGMENTATION AS A BARRIER TO MODERNIZATION

The costs of fragmentation extend beyond audits. Governments at all levels are investing in cloud adoption, data modernization, and AI-enabled services. These initiatives depend on secure, interoperable systems and the ability to move through procurement and authorization processes efficiently.

A fragmented compliance environment complicates these efforts by limiting evidence reuse, introducing inconsistent expectations, and slowing time-to-authority.

Harmonization is not a constraint on modernization. It is a prerequisite for it.

THE COMPLIANCE ECOSYSTEM

A substantial professional ecosystem has developed around navigating regulatory complexity, including assessors, consultants, and framework-specific advisory services. These actors provide real expertise and value.

Harmonization does not eliminate this work; it reallocates it. Reduced administrative duplication enables security professionals to focus on complex, high-value risk management challenges rather than reconciling avoidable differences across frameworks that share the same technical foundation.

Section 2: Emerging Federal Direction and the Path Forward

A SHIFT ALREADY UNDERWAY

Recent federal initiatives reflect growing recognition that the current cybersecurity compliance model is both costly and addressable. Efforts such as FedRAMP modernization, including increased automation and structured evidence approaches, and adjustments to NIST Rev. 5 implementation reflect meaningful movement toward greater efficiency and interoperability.

These initiatives demonstrate a shift away from narrative-heavy, point-in-time compliance models toward machine-readable evidence and continuous authorization concepts. Standardized data formats and automation reduce administrative overhead and create the technical conditions necessary for evidence reuse across programs — a foundational requirement for any reciprocity-based model.

Similarly, the evolution of the U.S. Department of Defense (DoD) Cybersecurity Maturity Model Certification (CMMC) reflects a renewed emphasis on verified compliance and continuous assurance. Movement away from self-attestation and toward phased, validated approaches reinforces the importance of demonstrable security outcomes grounded in well-defined standards.

Taken together, these efforts signal federal willingness to modernize how cybersecurity assurance is performed. However, deployed independently — without a harmonized policy framework — they cannot fully deliver on their potential.

Harmonization provides the connective tissue that allows these initiatives to scale across programs rather than remain siloed within them.

BUILDING ON PRIOR ADMINISTRATIONS' WORK

The policy foundation for harmonization has been established over multiple administrations, providing a strong and persistent basis for execution.

Key milestones include:

- **GAO-20-123 (2020):** Identified significant duplication and conflicting requirements across federal programs and issued twelve recommendations for improved coordination, including direction to OMB to strengthen interagency collaboration. This study remains the most comprehensive baseline assessment of the problem.

- **National Cybersecurity Strategy (2023) and Implementation Plan:** Explicitly identified regulatory harmonization as a strategic objective and assigned ONCD a coordination role. Subsequent updates added initiatives exploring reciprocity pilots and aligned reporting approaches.

- **National Security Memorandum-22 (April 2024):** Directed DHS to develop a harmonization plan as part of the National Infrastructure Risk Management Plan, establishing a formal interagency obligation to advance alignment.

- **CIRCIA Cyber Incident Reporting Council (September 2023):** Documented fifty-two distinct federal reporting requirements and recommended standardized definitions, timelines, and triggers — providing a concrete example of what practical harmonization outputs can look like.

Participants at the Symposium were clear: the analytical groundwork has been laid, the policy intent articulated, and the opportunity now is to move from initiation to execution.

THE PRIMARY MECHANISM: OMB-LED RECIPROCITY

Across discussions, participants consistently identified **OMB guidance establishing formal reciprocity** as the single highest-impact near-term action available under existing authority.

Under this model, OMB — in coordination with ONCD — would issue guidance establishing that compliance with one sufficiently rigorous federal cybersecurity framework satisfies equivalent requirements in another. This would apply both to federal agencies and to state and local governments subject to multiple federal programs.

Initial scope could focus on frameworks with the highest documented overlap, including CJIS, IRS Publication 1075, CMS, SSA, and FedRAMP. The guidance would define conditions for evidence reuse, establish expectations for mutual recognition, and create a formal process for resolving genuinely divergent requirements.

This approach is not novel. GovRAMP already applies a similar model by recognizing FedRAMP authorizations as satisfying equivalent baseline requirements. The Symposium discussions affirmed that extending this logic government-wide is both technically feasible and operationally impactful.

Participants frequently cited an existing analogy: states already recognize driver's licenses issued by other states without re-testing each driver at every state line. A comparable trust architecture for cybersecurity assessments — founded on shared standards and accountability — would produce immediate, measurable benefits.

GOVRAMP'S ROLE

GovRAMP does not seek to replace federal standards or position itself as the framework to which others must align. Instead, GovRAMP provides a working, operational model for how reciprocity, shared baselines, and coordinated governance can function across state and local environments.

GovRAMP's role in federal harmonization efforts is intentionally supportive:

- Providing tested approaches to evidence reuse and baseline alignment
- Offering crosswalk tools grounded in NIST SP 800-53
- Supporting structured engagement between federal agencies and SLTT stakeholders
- Demonstrating at scale that shared-baseline authorization models can operate effectively across jurisdictions

State associations, including NASCIO, have emphasized harmonization as a federal advocacy priority — specifically calling for OMB coordination authority, consistent interagency collaboration, and meaningful inclusion of state CIO and CISO perspectives. GovRAMP's work is designed to complement these priorities by translating federal policy direction into operational capability.

Looking ahead, GovRAMP is well positioned to support federal pilots and demonstrations — particularly in coordination with FedRAMP modernization efforts — illustrating how federal-state reciprocity can be implemented without lowering standards or increasing risk.

At its core, GovRAMP's approach aligns with the principle guiding this paper: the objective is not a single framework, but a shared foundation that allows evidence produced once to satisfy requirements across many.

Section 3: Policy Path Forward

Addressing cybersecurity regulatory fragmentation will require coordinated, sustained action across federal leadership, with meaningful engagement from state and local governments and the private sector. The recommendations below reflect the consensus that emerged from the 2026 GovRAMP Symposium and are grounded in existing analysis, prior harmonization efforts, and current federal authorities.

They are organized around a central objective — establishing reciprocity anchored in shared baselines — and the supporting actions necessary to make that objective durable and operational.

FOR OMB AND ONCD

1. Issue Formal Reciprocity Guidance

The Office of Management and Budget (OMB), in coordination with the Office of the National Cyber Director (ONCD), should issue formal guidance establishing that compliance with one sufficiently rigorous federal cybersecurity framework satisfies equivalent requirements in another.

This guidance should apply both to federal agencies and to state and local governments subject to multiple federal frameworks. Initial implementation should focus on frameworks with the highest documented overlap and operational impact, beginning with CJIS, IRS Publication 1075, CMS, SSA, and FedRAMP. GovRAMP should align to support those serving SLED/SLTT who must demonstrate conformance to these requirements.

The guidance should:

- Define the conditions under which evidence reuse is permissible
- Establish expectations for mutual recognition
- Specify a process for resolving cases involving genuinely divergent requirements

This action can be advanced under existing authority and would produce immediate reduction in duplication without weakening security standards.

2. Reconvene an Interagency Harmonization Working Group to Produce a Common Baseline

Building on prior mandates under National Security Memorandum-22 and GAO recommendations, OMB should reconvene an interagency harmonization working group charged with producing a common baseline control set and a formal framework for mutual recognition.

The working group should include OMB, ONCD, CISA, NIST, GSA, and sector-specific agencies with jurisdiction over high-overlap programs. Its mandate should include:

- Defining a shared NIST SP 800-53 baseline
- Establishing governance mechanisms for maintaining alignment over time
- Providing public progress reporting to support accountability and stakeholder confidence

Engagement with operational partners — including organizations such as GovRAMP — will be critical to ensuring outcomes are implementable in practice.

3. Advance External Framework Leveraging Through FedRAMP Modernization

GSA, through the FedRAMP Program Management Office and in coordination with OMB, should continue advancing efforts to evaluate how external frameworks and existing authorizations can be leveraged to streamline cloud authorizations and reduce duplicative assessments.

Recent FedRAMP modernization initiatives, including exploration of alternative authorization pathways and improvements to Rev. 5 balance, present near-term opportunities to pilot reciprocity-based approaches without abandoning established assurance models.

Progress in this area should be coordinated with OMB-led reciprocity guidance and informed by operational pilots that demonstrate how structured evidence from programs such as GovRAMP can support efficient authorization while maintaining rigorous security outcomes.

FOR CONGRESS

4. Request an Updated GAO Harmonization Review

Congress should request that the Comptroller General conduct an updated review of federal cybersecurity regulatory harmonization, building on GAO-20-123 and subsequent assessments.

This review should evaluate:

- Progress made since prior recommendations
- Remaining barriers to reciprocity and alignment
- Whether additional legislative authority is needed to advance mutual recognition or address demonstrably redundant requirements

An updated GAO review would provide an independent assessment to inform both oversight and future legislative action.

5. Expand CIRCIA's Harmonization Council to Include SLTT Representation

Congress should consider expanding the mandate of CIRCIA's Cyber Incident Reporting Council to formally include state, local, tribal, and territorial (SLTT) representatives.

Including CIOs, CISOs, chief privacy officers, and compliance leaders from SLTT governments would strengthen harmonization outputs by ensuring they reflect the realities of implementation across jurisdictions.

6. Ensure Adequate Resourcing for Harmonization Efforts

Interagency harmonization efforts require sustained leadership, staffing, and analytical support. Congress should ensure that whichever entity is tasked with leading this work has the authority and resources necessary to complete it.

This includes considering whether existing funding vehicles — such as the State and Local Cybersecurity Grant Program — could be leveraged to support SLTT participation in harmonization development and implementation.

FOR STATE AND LOCAL GOVERNMENTS

7. Engage Actively in Federal Harmonization Processes

State CIOs and CISOs are uniquely positioned to inform harmonization efforts through direct implementation experience. Active engagement — through federal working groups, public comment processes, and professional associations — is essential to ensuring that policy outputs are operationally viable.

Formalized engagement mechanisms, including those convened by GovRAMP and state associations, strengthen the practitioner voice and improve the quality and durability of harmonization outcomes.

FOR THE PRIVATE SECTOR

8. Invest in Structured Evidence Infrastructure

Cloud service providers serving both federal and SLTT markets should continue investing in structured, machine-readable evidence formats, including OSCAL-based documentation.

As authorization programs increasingly move toward standardized evidence reuse, vendors with mature structured evidence practices will be best positioned to demonstrate compliance across multiple frameworks from a shared evidence base — realizing the full benefit of the "do once, use many" model.

Recommendations: Summary Table

The following table summarizes each recommendation, the entity best positioned to advance it, and an indicative timeframe.

#	Recommendation	Responsible Party	Timeframe	Key Outcome
1	Issue OMB Reciprocity Guidance	OMB / ONCD	Near-term priority	Formal guidance that compliance with one rigorous federal framework satisfies equivalent requirements in another. Initial scope: CJIS, IRS 1075, CMS, SSA, FedRAMP; offer guidance on how to leverage GovRAMP or other authorizations at SLED/SLTT intersection as well
2	Reconvene Interagency Harmonization Working Group	OMB / ONCD	Initiate within 12 months	Charge an interagency body with producing a common baseline and mutual recognition framework within 12 months, with public progress reporting.
3	Advance External Framework Leveraging through FedRAMP x Modernization	GSA / OMB	Near-term	Expanded use of external frameworks to reduce duplication and enable more efficient authorization pathways, with pilots informing future policy decisions on broader reciprocity.
4	Direct an Updated GAO Harmonization Review	Congress	Current Congress	Assess progress since GAO-20-123 and GAO-24-107602, identify remaining barriers, and determine authority needed to mandate reciprocity.
5	Expand CIRCIA Harmonization Council to Include SLTT	Congress	Next legislative vehicle	Formally include state and local officials so harmonization outputs are implementable at the state level.
6	Publish Interagency Crosswalk (CJIS, IRS 1075, CMS, SSA, FedRAMP)	Sector agencies / NIST	12–18 months	A living crosswalk to a common NIST SP 800-53 baseline with mutual recognition guidance. GovRAMP will publish its own crosswalk as a working model.

Conclusion

The current cybersecurity compliance landscape is characterized by fragmentation that drives cost, complexity, and inefficiency across government and industry. At the same time, the United States is entering a critical period of government modernization — one that depends on secure, interoperable systems and scalable infrastructure.

Harmonization offers a clear path forward. By advancing shared baselines, enabling evidence reuse, and fostering coordination across agencies and levels of government, federal leadership can help build a more unified and efficient cybersecurity ecosystem — one that strengthens security outcomes without multiplying the burden on the organizations responsible for delivering them.

The analytical work has been done. The policy direction has been established. GovRAMP, together with its state and local partners, stands ready to support the operational and convening work needed to turn that direction into durable results.

This is not simply a compliance issue — it is a strategic opportunity to improve the efficiency, security, and modernization capacity of government at every level.

Appendix A: About The Symposium

The 2026 GovRAMP Symposium was held March 9, 2026 at the Ronald Reagan Building, Washington D.C., in coordination with the Billington State & Local CyberSecurity Summit. The Symposium convened senior leaders from federal and state government, Congress, the private sector, and the cybersecurity community to examine opportunities for advancing regulatory harmonization across the federal-state ecosystem.

Agenda:

10:30 – 11:30 am | PRIVATE SESSION: Federal Cyber Harmonization — Fireside Chat with Congressional Leadership/Staff

11:30 – 12:30 pm | Registration Check-In & Buffet Lunch

12:30 – 12:40 pm | Welcome Remarks — Leah McGrath, GovRAMP Executive Director & Joe Bielawski, President, Knowledge Services

12:40 – 1:30 pm | Regulatory Harmonization as a Catalyst for Innovation and National Security — Panel | Moderator: Teri Takai, e.Republic

1:35 – 2:20 pm | From Guardrails to Green Lights: A New Cyber Playbook for the AI Era — Keynote Panel | Moderator: Leslie Anderson, MITRE

2:20 – 2:35 pm | Networking Break

2:35 – 3:20 pm | How to Achieve Regulatory Harmonization — Interactive Workshop

3:20 – 3:30 pm | Final Thoughts: AI, Cyber, and the Regulatory Horizon — Tony Sauerhoff, Chief AI & Innovation Officer and State CIO & Executive Director, Texas DIR

4:00 pm | Fireside Chat with ONCD Director Sean Cairncross — Billington State & Local CyberSecurity Summit

Appendix B: About GovRAMP

GovRAMP is a nonprofit 501(c)(6) membership organization operating a cybersecurity authorization program designed for state and local governments. GovRAMP uses NIST SP 800-53 as its foundational control catalog — the same baseline that underlies FedRAMP and the major federal sector-specific frameworks — and currently treats FedRAMP authorization as a recognized pathway into the GovRAMP program.

This design reflects the same reciprocity principle this paper advocates at the government-wide level: rigorous work performed under one framework should be recognized by another, rather than repeated from scratch. GovRAMP's Progressing Security Snapshot (PSP) program extends this further, providing continuous monitoring of authorized cloud service providers and offering a practical state-level model for the shift from point-in-time to continuous authorization.

GovRAMP does not seek designation as a federal standard. GovRAMP's role in the broader harmonization effort is operational and convening: publishing crosswalk tools, supporting state and local participation in federal policy processes, and demonstrating at scale that shared-baseline, reciprocity-based authorization is achievable.

Appendix C: Key References

- GAO-20-123: Cybersecurity: Selected Federal Agencies Need to Coordinate on Requirements and Assessments of States (May 2020)
- GAO-24-107602: Cybersecurity: Efforts Initiated to Harmonize Regulations, but Significant Work Remains (June 2024)
- National Cybersecurity Strategy (March 2023) and Implementation Plan (July 2023; Version 2, May 2024)
- National Security Memorandum-22 on Critical Infrastructure Security and Resilience (April 2024)
- DHS Harmonization of Cyber Incident Reporting to the Federal Government (September 2023)
- ONCD Request for Information on Cyber Regulatory Harmonization (August 2023)
- FedRAMP 20X program updates, pilots, and Requests for Comment (Ongoing)
- NASCIO Federal Advocacy Priorities: nascio.org/government-affairs/federal-advocacy-priorities/

Appendix D: Glossary

Common Baseline: A formally curated subset of NIST SP 800-53 controls recognized by multiple frameworks as satisfying the foundational security requirement, with program-specific overlays built on top. Enables evidence produced under the baseline to satisfy requirements across programs without repeated assessment.

Control Parameters: Specific values that NIST SP 800-53 requires agencies to define when tailoring security controls to their programs — such as failed login attempt thresholds or audit log retention periods. Conflicting parameters across agencies are the primary driver of duplicative compliance burden for state and local governments.

Mutual Recognition / Reciprocity: A formal agreement that compliance with one framework satisfies equivalent requirements in another, enabling evidence reuse and reducing duplicative assessment.

NIST SP 800-53: The NIST security and privacy controls catalog serving as the common foundational baseline for FedRAMP, GovRAMP, CJIS, IRS 1075, CMS, and SSA frameworks.

OSCAL: Open Security Controls Assessment Language. A machine-readable format developed by NIST to standardize security control information, enabling automated assessment and cross-framework mapping.

FedRAMP: Federal Risk and Authorization Management Program. U.S. government-wide cloud security assessment and authorization program.

GovRAMP: A nonprofit 501(c)(6) state and local government cloud security authorization program using NIST SP 800-53 as its foundational control catalog.

SLTT: State, local, tribal, and territorial governments.

ONCD: Office of the National Cyber Director. White House office responsible for national cybersecurity strategy coordination.

CIRCIA: Cyber Incident Reporting for Critical Infrastructure Act (2022). Established an interagency body to harmonize federal cyber incident reporting requirements.

Appendix E: Methodology Note

This document was prepared by GovRAMP staff using structured notes from the 2026 Symposium, supplemented by written input from panelists and participants. It represents a synthesis of discussion and does not constitute the formal policy position of GovRAMP, any participating agency, speaker, or organization. Draft sections were circulated for factual review before publication.

Appendix F: Companion Document – Record of Symposium Discussion

This white paper is one of two companion documents produced from the 2026 GovRAMP Symposium. It presents the policy analysis, context, and recommendations that emerged from the day's discussions.

The companion document — ***Cyber Harmonization as a National Security Strategy: Post-Symposium Findings Report*** — provides an extended record of the discussions held across each Symposium session, including the private meeting, the two main panels, and the interactive workshop. It is intended to serve as a fuller narrative account of the themes, exchanges, and areas of consensus that shaped the conclusions presented in this document. Readers seeking additional context for any recommendation in this paper are encouraged to consult the companion document for the underlying discussion that informed it.

Both documents were prepared by GovRAMP staff and are intended to be read together. The white paper sets the policy direction; the companion record preserves the practitioner voices and deliberative process behind it.

GOVRAMP.ORG | INFO@GOVRAMP.ORG | LINKEDIN.COM/COMPANY/GOVRAMP