GovRAMP

Version 1.0

2026 GovRAMP Symposium on Framework Harmonization

Findings and Discussion Record

March 9, 2026

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

Document Overview

PURPOSE

This document provides a session-by-session record of the discussions held at the 2026 GovRAMP Symposium. It captures the themes, perspectives, and areas of consensus that emerged throughout the day, without advancing independent policy prescriptions.

The intent is to preserve the practitioner context behind the Symposium's conclusions and to serve as a companion to the formal GovRAMP policy white paper. Together, the two documents reflect both the what and the why of the policy direction that emerged from the Symposium.

SCOPE

The 2026 GovRAMP Symposium convened senior leaders from federal and state government, Congress, industry, and the cybersecurity community to examine a central strategic question:

How can the United States harmonize cybersecurity regulatory requirements to accelerate government modernization — including AI adoption — while strengthening national security?

Discussions focused on three interconnected dimensions of that challenge:

- Framework harmonization: Reducing duplication and friction across NIST, FedRAMP/GovRAMP, Department of Defense, and sector-specific regulatory regimes
- AI-era cyber policy: Developing assurance and governance models capable of keeping pace with AI-enabled systems
- Intergovernmental coordination: Aligning federal, state, and local approaches to create a more coherent national security posture

AUTHORS AND CONTRIBUTORS

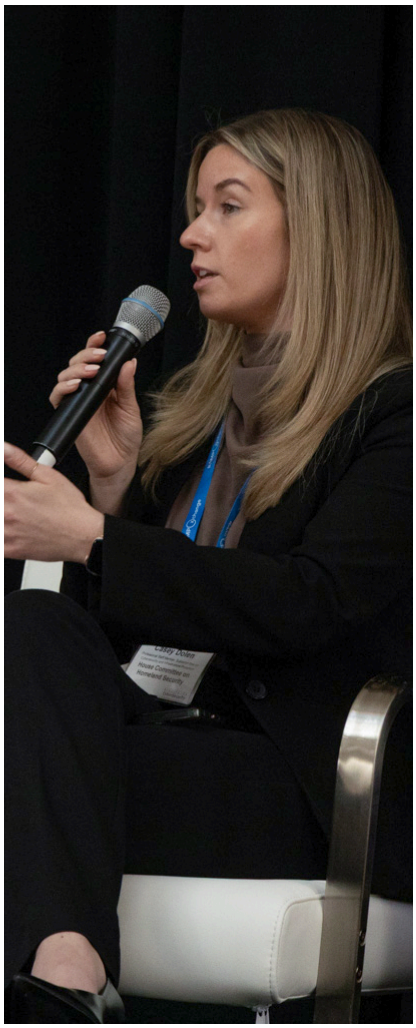
This document was prepared by GovRAMP staff, drawing on structured notes and post-event input from Symposium participants. It reflects a synthesis of discussion and does not represent the formal position of any individual speaker, agency, or organization.

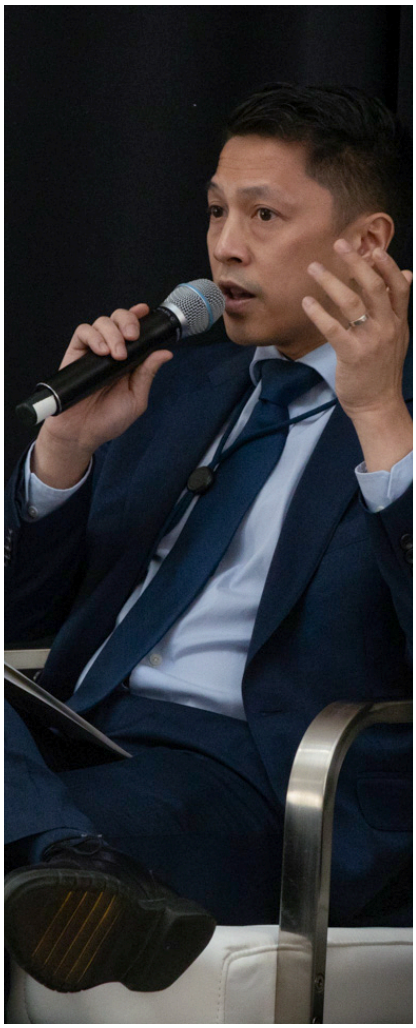
HOW TO USE THIS DOCUMENT

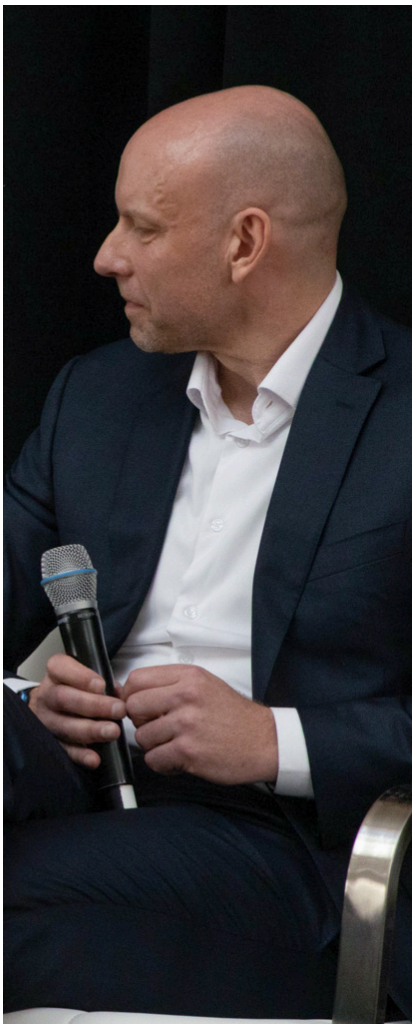
The document follows the Symposium agenda, with each major session mapped to a corresponding section.

This record is one of two companion products from the 2026 GovRAMP Symposium. It captures the deliberative discussion and practitioner insights that informed the event. The companion white paper — ***Cybersecurity Harmonization as a National Security Strategy: Policy White Paper & Post-Symposium Conclusions*** — presents the resulting policy analysis and recommendations.

Readers are encouraged to consult both documents together: this record provides context and grounding; the white paper translates that context into actionable policy direction.







Executive Summary

The United States faces a growing strategic paradox. While it continues to lead globally in the development of cloud, AI, and cybersecurity technologies, its own public-sector digital modernization is increasingly constrained by a fragmented and duplicative compliance environment. Overlapping cybersecurity frameworks slow procurement, divert scarce security talent from operational defense, and create unnecessary barriers for innovative vendors — without delivering commensurate security gains.

The 2026 GovRAMP Symposium convened to examine this challenge directly and to identify realistic paths forward. Across panels, workshops, and private leadership sessions, participants converged on a shared conclusion: **regulatory fragmentation is no longer a compliance inconvenience — it is a national security risk**.

The cost of inaction is strategic. Fragmented requirements delay modernization, complicate AI adoption, and weaken the government's ability to respond at speed to evolving threats. This report summarizes the core themes and insights that emerged during the Symposium discussions and provides context for the policy recommendations presented in the companion white paper.

Notably, during the Symposium, the National Association of State Chief Information Officers (NASCIO) invited all interested organizations to join its government affairs work on this issue, including to co-host a follow-up convening with GovRAMP. This commitment reflects the Symposium's central takeaway: progress will be driven by coalition-building, practitioner engagement, and sustained coordination — not by compliance mandates alone.

KEY TAKEAWAYS AT A GLANCE

- **Regulatory fragmentation is a national security problem.** The United States maintains dozens of overlapping cybersecurity frameworks that force cloud vendors, state agencies, and contractors to duplicate compliance efforts without proportionate improvements in security. The result is slower modernization and misallocated security resources.

- **A common baseline is the most viable near-term path forward.** Participants across all sessions converged on establishing a shared, NIST-grounded baseline as the most actionable initial step. This approach reduces duplication while preserving the ability for programs to retain justified overlays.

- **Certain federal frameworks should be prioritized for harmonization.** CJIS, IRS Publication 1075, SSA, and CMS were identified as the highest-impact candidates for initial engagement due to their broad and overlapping reach across state, local, tribal, and territorial governments. This aligns with prior U.S. Government Accountability Office (GAO) findings documenting both the cost and prevalence of conflicting requirements across these programs.

- **Trust — not technology — is the primary barrier.** Governments already practice mutual recognition in other domains. The Symposium made clear that the challenge in audit and evidence reuse is not technical feasibility, but the absence of formal trust and reciprocity mechanisms between regulatory owners.

- **AI governance is the forcing function.** AI is already operational in government. Fragmented compliance environments are now among the largest structural barriers to responsible, competitive AI adoption. In this context, cyber harmonization is AI policy.

- **States are ready to lead.** State CISOs, CIOs, and government executives expressed a strong appetite to move faster than federal mandates allow. A coalition-driven approach — led in part by states — emerged as the most realistic engine for near-term progress.

THE CENTRAL ARGUMENT

Cybersecurity regulatory harmonization is not a matter of convenience; it is a strategic imperative. The United States cannot maintain its leadership in effective, secure government if agencies and vendors are forced to navigate dozens of overlapping and sometimes contradictory frameworks.

Harmonization reduces friction, accelerates procurement, and allows the nation's cyber workforce to focus on managing real risk rather than producing duplicative documentation. Done correctly, it strengthens — rather than weakens — security outcomes.

Section 1: Framework Harmonization as an Innovation Catalyst

Regulatory Harmonization as a Catalyst for Innovation and National Security

This opening panel examined how aligning cybersecurity frameworks — including National Institute of Standards and Technology (NIST), FedRAMP, GovRAMP, U.S. Department of Defense requirements, and sector-specific regimes — can strengthen national security while accelerating government adoption of cloud, AI, and emerging technologies.

The discussion focused not on whether existing frameworks are necessary, but on whether the way they are administered today supports or undermines the outcomes they are designed to achieve.

THE PROBLEM: REGULATORY FRAGMENTATION

The current cybersecurity regulatory environment reflects decades of well-intentioned policy development undertaken largely in silos. The result is a patchwork of overlapping frameworks that organizations must navigate simultaneously.

Cloud providers seeking to serve federal agencies, state and local governments, defense contractors, and regulated sectors routinely face requirements that:

- Duplicate assessment and documentation efforts without delivering proportional security gains
- Consume limited cybersecurity talent on compliance administration rather than active risk reduction
- Create procurement barriers that disproportionately affect smaller and innovative vendors
- Slow the adoption of AI and other emerging technologies across government

Panelists emphasized that fragmentation is most acute for vendors operating across both federal and state markets. Many cloud providers maintain separate commercial and government product lines primarily to satisfy differing compliance expectations — even when the underlying technical controls are substantially similar.

The FBI's Criminal Justice Information Services (CJIS) requirements emerged as a frequently cited example. Historically, CJIS data-location mandates drove agencies toward government-specific cloud environments. As commercial cloud platforms have evolved to support U.S.-only data residency through configuration controls, the technical justification for separate product tracks has diminished — yet compliance expectations have not kept pace. The result is parallel assessment processes with near-identical control requirements, separate auditors, and duplicative costs.

DISCUSSION HIGHLIGHTS

The panel, moderated by Teri Takai, featured Victoria Yan Pillitteri (NIST), Bernice Russell-Bond (North Carolina CISO), Nick Leiserson (Institute for Security and Technology), and Casey Dolen (House Committee on Homeland Security).

Across the discussion, there was broad agreement that the proliferation of cybersecurity frameworks is a solvable problem — and that solving it does not require selecting a single "winner." As Pillitteri framed it, the challenge is not whether one framework should replace others, but how existing frameworks can work together for the practitioners responsible for implementation.

Dolen highlighted growing congressional attention to regulatory alignment, particularly in the context of the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), which established an interagency mechanism to deconflict incident reporting requirements. GAO's parallel review of more than 50 incident reporting mandates across 40 federal agencies further illustrates the scale of the problem and the growing demand for coordination.

Russell-Bond offered the operational perspective from the state CISO seat: the issue is not that individual frameworks are unreasonable, but that meeting multiple frameworks simultaneously is unsustainable. In highly regulated environments, a significant share of cybersecurity budgets is consumed by documentation, audits, and assessment preparation rather than by threat detection and response.

Leiserson reinforced a distinction that surfaced repeatedly throughout the Symposium: **compliance and security are not the same thing**. Effective risk management produces security outcomes; compliance should be a byproduct of that work. A regulatory environment that rewards documentation over risk reduction ultimately undermines its own objectives.

THE FEDERAL–STATE DYNAMIC

State governments sit at the intersection of nearly every federal cybersecurity framework — CJIS, IRS Publication 1075, CMS requirements, and others — while also managing state-specific statutory requirements and constrained resources.

The private session with state CISOs and CIOs made this burden tangible. Smaller counties and municipalities may have one or two IT staff, no dedicated security leadership, and limited ability to interpret hundreds of pages of controls — yet they face the same expectations for data protection as far larger entities.

Even large state agencies face structural challenges. Different agencies within the same state government may be subject to different federal frameworks, preventing the development of a unified and cost-effective enterprise security program. As one state CIO noted, the primary challenge is not differing security practices, but differing interpretations and evidence submission requirements for controls that are often substantively identical.

The consistent ask from state leaders was not to lower standards, but to align them — so that evidence produced once can be reused across multiple programs.

THE NIST PERSPECTIVE

Victoria Yan Pillitteri described NIST's role as an increasingly important translational function across frameworks rather than as the owner of a single authoritative standard.

NIST is actively advancing work across multiple fronts — including the Privacy Framework, AI overlays for SP 800-53, the Cybersecurity Framework AI Profile, FIPS 200 updates, and SP 800-172. The volume of parallel activity underscores the challenge: maintaining coherence across an expanding portfolio while responding to rapidly evolving threats and technologies.

Pillitteri emphasized that the core strength of most frameworks lies in their underlying scope. The challenge for practitioners is understanding how one framework translates to another. NIST's priority is making those translations clearer and more usable, not mandating consolidation.

Participants also noted that developments such as the FedRAMP 20X rulemaking — which signals openness to recognizing external frameworks that meet the majority of FedRAMP requirements — represent meaningful movement toward formal equivalency and mutual recognition, an area where GovRAMP remains actively engaged.

SECTION 1 KEY FINDINGS

Finding 1.1:
High compliance cost is not an indicator of strong security. It signals misalignment between regulatory intent and operational reality and diverts scarce resources away from risk reduction.

Finding 1.2:
The problem is not the existence of multiple frameworks, but the lack of coordination among them. Individual frameworks serve legitimate purposes; the absence of formal mechanisms for evidence reuse and mutual recognition is the core deficiency.

Finding 1.3:
Legislative and oversight momentum exists, but practitioner engagement is essential. Without operational input, harmonization mandates risk producing technically correct but unworkable outcomes.

Finding 1.4:
The federal–state dynamic is structurally asymmetric. States receive federal requirements as mandates without corresponding alignment across agencies, creating confusion and inconsistent administration. Any harmonization strategy that ignores this reality will fail at implementation.

Finding 1.5:
Conflating compliance with security is counterproductive. Harmonization efforts must prioritize real risk management outcomes, not simply reduced paperwork.

Section 2: How to Achieve Regulatory Harmonization

How to Achieve Regulatory Harmonization

This session moved the Symposium from problem framing to solution design. Facilitated by Teri Takai (e.Republic), Leslie Anderson (MITRE), and Katerina Megas (NIST), the workshop evaluated four distinct pathways for achieving cybersecurity regulatory harmonization.

Participants assessed each option against feasibility, impact, political viability, and implementation complexity, drawing on real-world experience managing and complying with multiple frameworks.

THE FOUR HARMONIZATION PATHWAYS

Option 1: Same Language

Clarifying how requirements map across frameworks

This pathway focuses on establishing shared terminology, definitions, and crosswalks that allow practitioners to understand how requirements in one framework correspond to requirements in another — without eliminating any program or requiring major regulatory change.

Workshop participants viewed “same language” as a foundational step for all other harmonization efforts. A consistent challenge identified across sectors is that frameworks often use different terminology to describe effectively identical controls, creating confusion and undermining confidence in crosswalks.

Without a shared taxonomy, even well-intended mappings are difficult to operationalize. Practitioners cannot reliably reuse evidence or assessments if they must reinterpret language each time they move between frameworks.

Participants emphasized that this approach requires sustained institutional ownership. A shared taxonomy must be actively maintained by NIST, CISA, and relevant sector agencies to remain authoritative and usable. Absent adoption incentives or expectations, shared language risks remaining aspirational rather than operational.

OSCAL was cited as an important partial implementation at the technical level, but participants stressed that semantic alignment at the policy level is equally critical.

Option 2: Common Baseline

Aligning programs to a shared foundational control set

The Common Baseline approach proposes that regulatory programs formally adopt a shared NIST-grounded baseline of security controls. Individual frameworks would retain justified overlays, but the foundational assessment could be performed once and reused across programs.

This option received the strongest support of any pathway evaluated. Participants consistently identified it as the **highest-impact and most politically feasible near-term strategy**.

The rationale is straightforward: most major cybersecurity frameworks already share a substantial common core. Divergence generally occurs at the overlay level, not in foundational expectations. Formalizing that shared foundation would reduce duplication while preserving program-specific needs.

Existing models demonstrate feasibility. GovRAMP's use of NIST SP 800-53 as its foundational control catalog and FedRAMP's impact-level structure both reflect baseline-and-overlay approaches in practice.

Participants acknowledged that the primary barriers are institutional, not technical. Program owners have significant investment in existing processes, and alignment requires a degree of shared governance and trust. There was also strong agreement that a common baseline must not become a lowest common denominator — harmonization must maintain or strengthen security requirements, not weaken them.

Option 3: Audit Harmonization

Reusing security assessments across programs

Audit harmonization applies the "test once, serve many" principle. Under this approach, a rigorous assessment performed for one authorization program would be formally recognized as satisfying equivalent requirements in others, eliminating the need for multiple audits of the same controls.

Participants identified audit harmonization as the pathway with the greatest potential for cost and time savings — and the one most dependent on institutional trust.

GovRAMP's recognition of FedRAMP authorizations was cited as a working example. Extending this model more broadly, however, presents challenges. Differences in audit scope, methodology, and authorized assessor pools create real — if sometimes overstated — barriers to reciprocity. Accountability structures within individual programs further complicate shared validation.

CJIS was frequently referenced as illustrative as a leader in aligning its security policy requirements to NIST 800-53, making it easier for common baselines across other frameworks. Participants noted that achieving audit reciprocity across other frameworks (such as SSA, CMS and IRS frameworks) would require formal agreements among program owners, alignment of assessor authorization requirements, and clear mechanisms for resolving cope gaps.

Option 4: Elimination

Consolidating frameworks under a single authority

Elimination — replacing multiple frameworks with one consolidated authoritative program — was viewed as the most structurally transformative option and the least viable in the near term.

Participants did not reject consolidation as an eventual goal, but they were clear-eyed about the requirements: congressional or executive action, significant interagency coordination, and multi-year transition planning. Institutional resistance from agencies and industries organized around existing frameworks would be substantial.

OSCAL was discussed as a potential technical enabler, but participants emphasized that technical interoperability does not resolve the governance question of ownership and accountability.

The consensus view was that elimination is a long-term destination. Progress on common baselines and audit harmonization is necessary to create the conditions under which consolidation could eventually succeed.

SECTION 2 KEY FINDINGS

Finding 2.1:
The four harmonization pathways are interdependent. Shared language enables common baselines; common baselines create conditions for audit reciprocity; audit reciprocity makes consolidation feasible. Progress can occur in parallel, but sequencing matters.

Finding 2.2:
A common baseline is the most effective near-term move. It offers meaningful reduction in duplication, preserves legitimate program differences, and establishes a foundation for broader reciprocity.

Finding 2.3:
Harmonization must strengthen security, not dilute it. Any baseline approach must meet or exceed the most rigorous participating requirements to avoid reducing outcomes to the lowest common denominator.

Finding 2.4:
Economic and institutional resistance is real. Assessment firms, consultants, and tooling vendors have grown around the current fragmented environment. Successful harmonization strategies must anticipate resistance and manage transitions without losing momentum.

Finding 2.5:
Incremental progress is more durable than comprehensive reform promises. Demonstrating real, achievable advances builds trust, expands coalitions, and creates momentum for larger reforms over time.

Section 3: Final Thoughts: AI, Cyber, and the Regulatory Horizon

Final Thoughts: AI, Cyber, and the Regulatory Horizon

Fireside Chat with Sean Cairncross, Director, Office of the National Cyber Director *(Billington State & Local Cybersecurity Summit)*

The closing sessions of the Symposium reinforced the day's central themes from an executive branch perspective and framed regulatory harmonization as an urgent issue of national competitiveness and security.

THE ONCD PERSPECTIVE

In his fireside chat, Sean Cairncross, Director of the Office of the National Cyber Director (ONCD), emphasized that the updated National Cybersecurity Strategy — released the Friday prior to the Symposium — explicitly identifies streamlined compliance and stronger public-private and intergovernmental partnerships as core strategic pillars.

This framing reflects a growing recognition at the administration level that fragmented cybersecurity requirements are not simply a compliance inconvenience. They impose real costs on innovation, slow modernization, and create structural disadvantages that adversaries do not face. Regulatory fragmentation functions as a tax on government speed — particularly in emerging technology domains where velocity matters.

Director Cairncross underscored that harmonization is not about weakening existing standards. It is about ensuring that regulatory structures enable secure adoption at the pace required to meet current threats.

AI AS THE FORCING FUNCTION

The ONCD perspective on artificial intelligence echoed a consistent message throughout the Symposium: **AI adoption in government is already underway**. The strategic question is no longer whether to deploy AI, but whether governance and assurance structures can support responsible deployment at competitive speed.

Existing cybersecurity frameworks provide an essential foundation, but they were not designed with AI-specific challenges in mind — including model drift, data provenance, algorithmic accountability, and the governance of AI-generated outputs in high-impact use cases.

The risk is asymmetric. Adversaries adopt AI capabilities immediately, without waiting for governance consensus. Government procurement and authorization processes, by contrast, can impose delays measured in years. Each delay extends the period during which AI systems operate without mature assurance frameworks — increasing operational and security risk rather than reducing it.

From this perspective, harmonization is not just cyber policy; it is AI policy. A fragmented regulatory environment is now one of the primary structural barriers to responsible AI adoption in government.

ADMINISTRATIVE ACTION VS. LEGISLATIVE AUTHORITY

The closing discussions also surfaced a productive tension between what can be accomplished through administrative action and what ultimately requires legislation.

From the executive branch perspective, significant progress is achievable without waiting for Congress. OMB guidance, FedRAMP rulemaking — including the 20X process — and interagency coordination offer near-term pathways to advance common baselines, shared taxonomy, and mutual recognition.

The legislative perspective, represented earlier in the day by House Homeland Security Committee staff, emphasized that durable harmonization requires accountability. Prior GAO recommendations and interagency taskings stalled due to the absence of statutory enforcement mechanisms and sustained oversight.

The emerging synthesis was pragmatic: progress should proceed immediately on achievable administrative actions, while legislative engagement focuses on creating the accountability structures, incentives, and resourcing needed to make that progress durable.

COALITION-LED PROGRESS

A recurring theme across the Symposium was the role of coalitions in driving momentum. Organizations such as GovRAMP and NASCIO were repeatedly cited as connective tissue — providing technical expertise, convening authority, and sustained practitioner engagement that individual agencies and legislative bodies often lack.

The bipartisan consensus around cybersecurity — noted by multiple speakers as a rare political advantage — creates a window for targeted action. That window will not remain open indefinitely. Demonstrated progress on achievable steps is essential to sustaining engagement and expanding participation.

INTERNATIONAL IMPLICATIONS

While the Symposium focused primarily on domestic regulatory alignment, several participants noted broader implications. Allied nations face similar challenges when navigating U.S. compliance requirements, and vice versa. A harmonized domestic environment would be more easily aligned with allied standards and strengthen U.S. leadership in international cybersecurity and AI governance forums.

Conversely, continued fragmentation weakens U.S. credibility in global standard-setting and creates openings for less rigorous — or adversary-designed — approaches to fill the gap.

STATE LEADERS PERSPECTIVE

Insights from the private morning session with state cybersecurity leaders reinforced and sharpened the themes surfaced publicly. State CISOs and CIOs were direct: they are prepared to lead on harmonization, but only with credible federal follow-through.

Prior harmonization efforts, including GAO recommendations and OMB taskings dating back more than six years, were not fully implemented. States are hesitant to invest in new harmonization infrastructure without confidence that federal commitments will be sustained.

State leaders emphasized that time matters. AI governance gaps are solidifying quickly, and delay risks locking in fragmented structures that will be difficult to unwind.

SECTION 3 KEY FINDINGS

Finding 3.1:
The National Cybersecurity Strategy explicitly frames streamlined compliance and partnership as national security priorities, providing executive-level support for harmonization efforts.

Finding 3.2:
AI adoption amplifies the urgency of harmonization. Governance frameworks are lagging deployment, increasing risk with every month of delay.

Finding 3.3:
Bipartisan consensus on cybersecurity is a strategic advantage and a perishable one. Targeted legislative action should take place while alignment exists.

Finding 3.4:
States are ready to lead but require credible, accountable federal commitment. Past failures have created justified caution among state actors.

Finding 3.5:
Demonstrated, incremental progress is more effective than comprehensive promises. Action on achievable steps creates the momentum necessary for broader reform.

Acknowledgments and Sponsors

ACKNOWLEDGMENTS

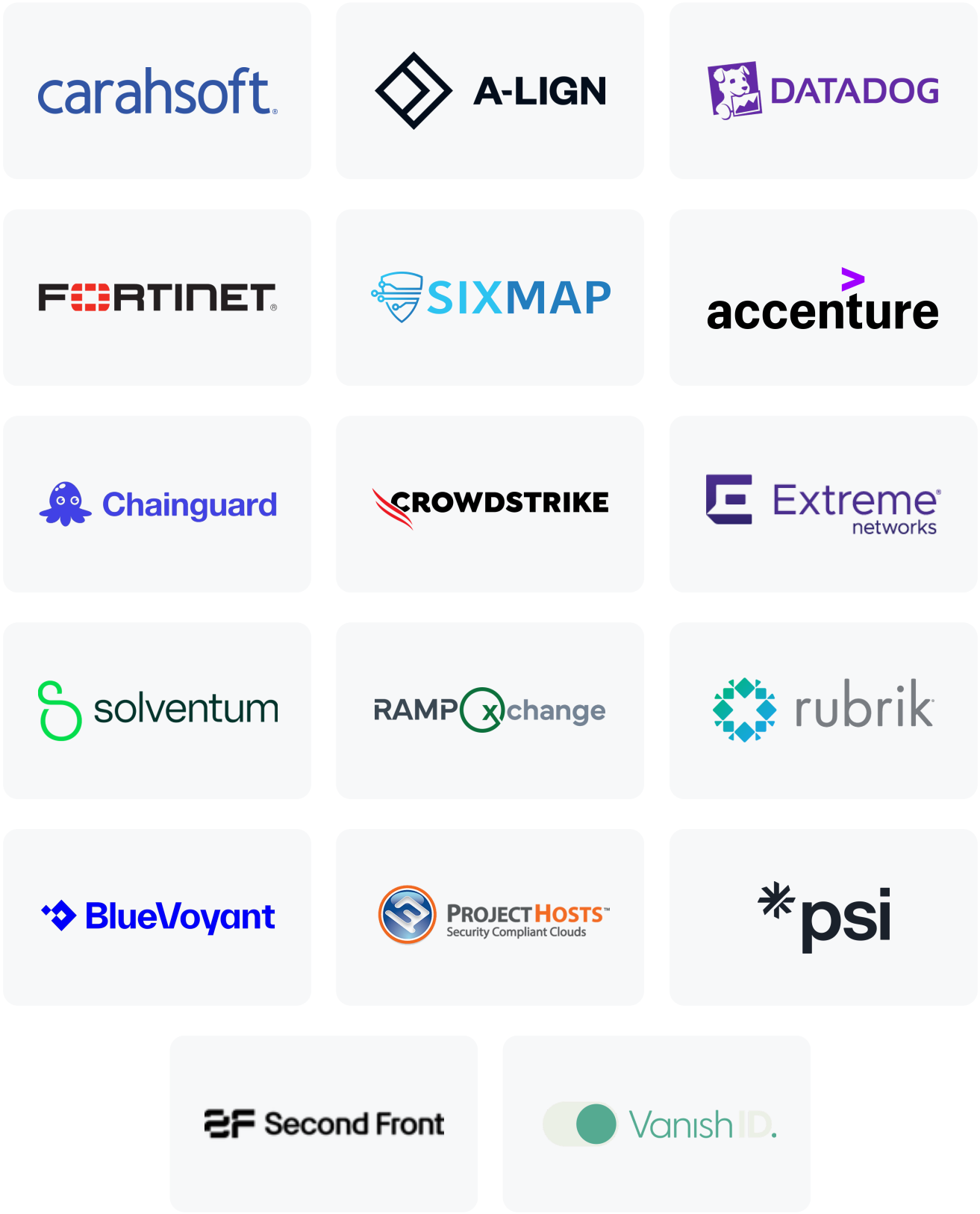
GovRAMP extends its sincere appreciation to the sponsors and partners whose support made the 2026 GovRAMP Symposium possible.

Their engagement enabled a substantive, practitioner-focused dialogue on cybersecurity regulatory harmonization at a critical moment for government modernization. Support for the Symposium reflected more than sponsorship — it demonstrated a shared commitment to strengthening security outcomes, reducing unnecessary compliance burden, and advancing collaboration across federal, state, and local government.

GovRAMP also gratefully acknowledges the leadership and contributions of its Board of Directors, committee members, task force participants, and the broader GovRAMP member community. Their ongoing involvement — through governance, advisory work, subject-matter expertise, and program participation — continues to shape and strengthen GovRAMP's ability to convene meaningful dialogue and advance practical solutions. While not all were able to attend the Symposium in person, their contributions are foundational to the work reflected in this report.

GovRAMP is thankful to all who support its mission and to those whose collective efforts help move cybersecurity regulatory harmonization from analysis to action.

2026 GOVRAMP SYMPOSIUM SPONSORS



Appendices

APPENDIX A: SYMPOSIUM AGENDA

2026 GovRAMP Symposium | March 9, 2026 | Ronald Reagan Building, Washington D.C.

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: GLOSSARY OF KEY TERMS

Cyber Harmonization
The process of aligning, consolidating, or establishing mutual recognition among overlapping cybersecurity regulatory frameworks to reduce duplication, lower compliance burden, and improve interoperability across government and industry.

FedRAMP
Federal Risk and Authorization Management Program (FedRAMP): a U.S. government-wide program providing a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

GovRAMP
GovRAMP is a nonprofit 501c6 membership organization built as an analogous program of FedRAMP for state and local governments, with increasing participation at the federal level as well.

NIST Cybersecurity Framework
A voluntary framework developed by the National Institute of Standards and Technology providing organizations with guidance to manage and reduce cybersecurity risk. NIST SP 800-53 provides the control catalog underlying FedRAMP and GovRAMP assessments.

OSCAL
Open Security Controls Assessment Language: a machine-readable data format developed by NIST to standardize how security control information is represented, enabling automated compliance assessments and framework mapping.

CMMC
Cybersecurity Maturity Model Certification: a DoW program requiring defense contractors to achieve specified cybersecurity standards as a condition of contract eligibility.

Mutual Recognition
A formal agreement between regulatory frameworks or jurisdictions that compliance with one framework satisfies equivalent requirements in another, enabling evidence reuse and reducing duplicative assessment effort.

APPENDIX C: NOTES ON METHODOLOGY

This document was prepared using a structured note-taking methodology during the Symposium, supplemented by written input solicited from panelists and participants following the event. Draft sections were circulated for factual review before publication. The document represents a synthesis of discussion and does not constitute the formal policy position of GovRAMP, any participating agency, or any individual speaker.

This document is a companion to the 2026 GovRAMP Symposium policy white paper: *Cybersecurity Harmonization as a National Security Strategy: Policy White Paper*. That document presents the policy recommendations and consensus positions that emerged from these discussions and includes a cross-reference to this record in its appendices (Appendix F). The two documents are intended to be read together.

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