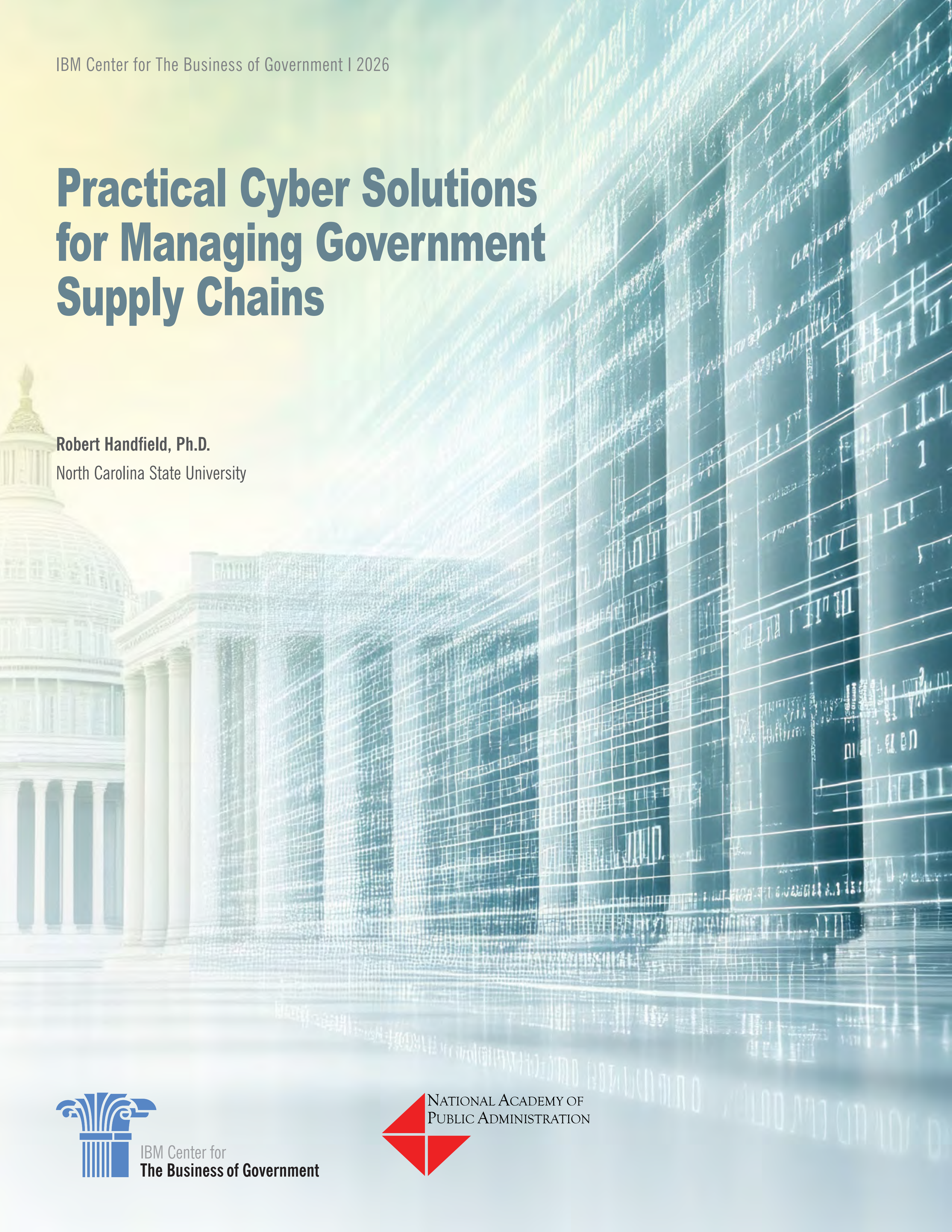
IBM Center for The Business of Government I 2026

Practical Cyber Solutions for Managing Government Supply Chains



Robert Handfield, Ph.D.
North Carolina State University

IBM Center for
The Business of Government

National Academy of
Public Administration

Practical Cyber Solutions for Managing Government Supply Chains

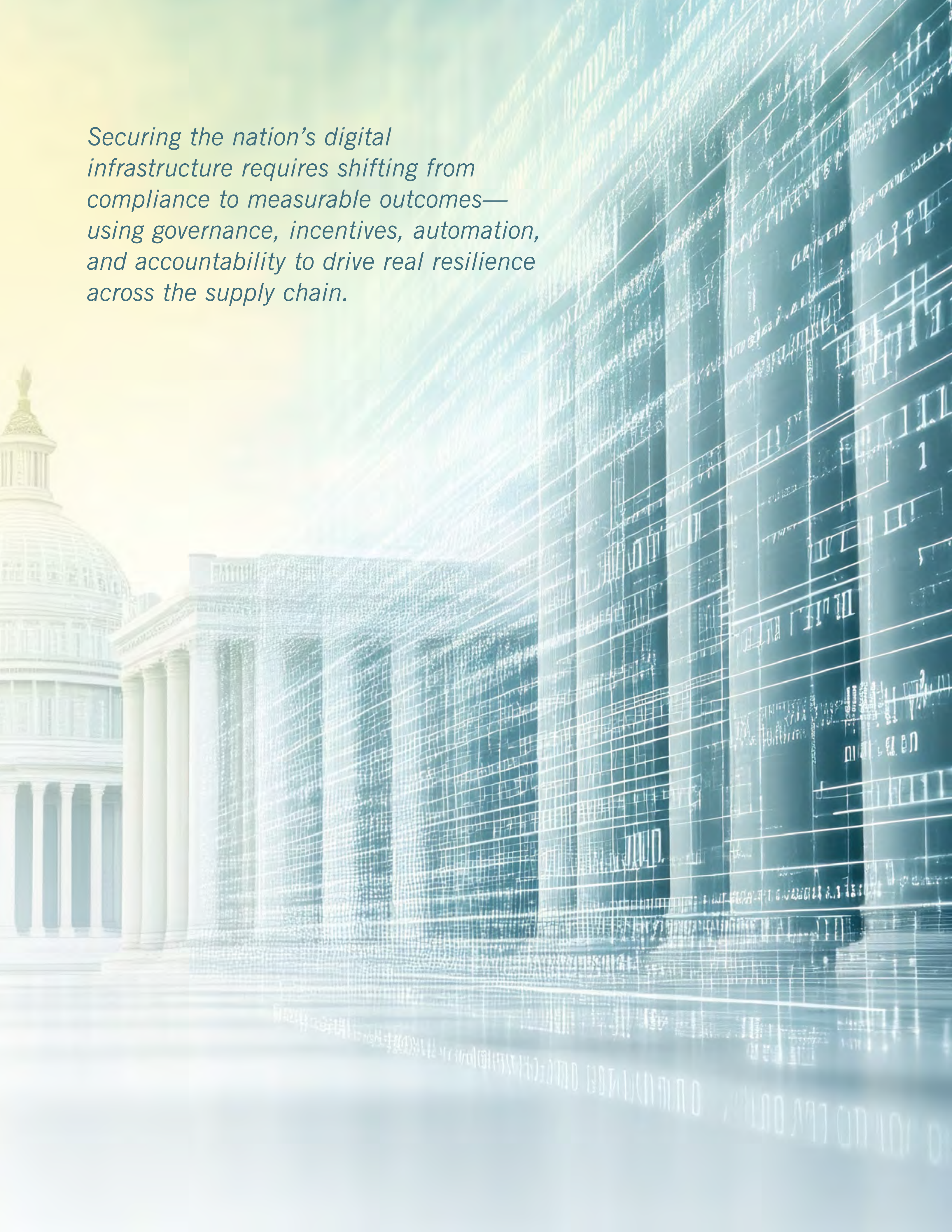
Robert Handfield, PhD
North Carolina State University

FEBRUARY 2026

IBM Center for
The Business
of Government

Table of Contents

Securing the nation's digital infrastructure requires shifting from compliance to measurable outcomes—using governance, incentives, automation, and accountability to drive real resilience across the supply chain.



Foreword

Public sector digital infrastructures face unprecedented and rapidly evolving threats. As government agencies work to secure complex, interconnected supply chains, the stakes for mission continuity, resilience, and public trust have never been higher. This new report, *Practical Cyber Solutions for Managing Government Supply Chains*, by Dr. Robert Handfield with North Carolina State University, offers a timely and actionable roadmap for strengthening Cybersecurity Supply Chain Risk Management (C-SCRM) across government.

Drawing on insights from a highlevel roundtable hosted by the IBM Center for The Business of Government and the National Academy of Public Administration, the report brings together experts from government, industry, and academia. Their discussions reflected a shared perspective that agencies can move beyond compliance-oriented approaches and embrace outcome-driven, secure-by-design practices that reduce risk, accelerate mitigation, and reinforce continuity of essential services.

Drawing on real-world experience, this report outlines practical steps the government can take to improve resilience—such as standing up centers of excellence, integrating risk-based cybersecurity measures, deploying AI-enabled diagnostics and remediation, and enhancing multi-tier supplier operations. These recommendations make clear that progress can emerge from an integrated strategy combining governance, metrics, automation, procurement levers, and cultural change.

This report builds on the IBM Center's longstanding commitment to advancing research at the intersection of technology, risk management, and public sector performance. Reports include *Enabling a More Resilient and Shared Supply Chain Strategy for the Nation: Lessons Learned from COVID-19*, *The Key to Modern Governmental Supply Chain Practice: Analytical Technology Innovation*, and *Improving Government Decision Making through Enterprise Risk Management*.

As agencies confront increasingly sophisticated adversaries, the guidance in this report provides leaders with a clear framework for action. By adopting the practices outlined here, government can strengthen operational readiness, protect essential services, and reinforce trust in the systems upon which the public depends. The analysis and recommendations presented by Professor Handfield—based on expert insights from the roundtable—offer strategic imperatives for applying cybersecurity for supply chain risk management across the public sector, and a practical path forward for building a more secure and resilient digital future.

Daniel J. Chenok
Executive Director
IBM Center for
The Business of Government
chenokd@us.ibm.com

Zoomie Zein
Partner, Finance &
Supply Chain Strategy &
Transformation. IBM
Zoomie.Zein@ibm.com

Executive Summary

The IBM Center for The Business of Government, in collaboration with the National Academy of Public Administration, recently hosted a roundtable discussion on "Practical Cyber Solutions for Managing Government Supply Chains." In this session, experts from government, industry, and academia came together to address the critical issues surrounding Cybersecurity Supply Chain Risk Management (C-SCRM).

The workshop convened senior leaders from federal agencies, industry, and academia to identify practical moves that harden the nation's digital infrastructure across three intertwined fronts:

1. Supply-chain security and acquisition
2. AI-enabled cyber defense and automation
3. Governance for resilience and future readiness

Participants emphasized that policy intent now exists to improve cybersecurity risk management for effective operation of supply chains involving government—but that execution gaps remain around contracting levers, metrics, talent, and cross-agency information-sharing.

Experts agreed that the government needs to move beyond a purely compliance-focused mindset on C-SCRM. The new focus should be on outcome-driven mission performance using contracts, incentives, continuous diagnostics, and transparent scorecards to reward secure-by-design vendors and to manage persistent underperformers. The discussions indicated that AI can be used proactively to accelerate threat detection, anomaly identification, vulnerability management, incident response, and C-SCRM. As generative and agentic AI have begun to be deployed in supply chain stress testing, organizations need to utilize these tools for scenario planning, supplier risk assessments, and disruption mapping—while assessing their organizational readiness in the areas of data quality, audits, and provenance.

Based on the discussion, agencies can move forward by starting now on ten top recommendations:

1. **Stand up a C-SCRM Center of Excellence (CoE)** as a shared service, with an executive dashboard and public-facing scorecards for selected measures, through the U.S. General Services Administration (GSA) or another lead agency.
2. **Launch a Secure-by-Design Vendor Merit Program,** with tiered incentives (such as preferred status or faster awards) and consequence management for repeated incidents.
3. **Deploy AI-driven Continuous Diagnostics and Remediation (CDR)** to automate triage (i.e., alerts, vulnerability mapping, and patch orchestration) and accelerate problem solving.
4. **Draft annual contract addenda to keep security obligations current** across multi-year service agreements, and track acknowledgment digitally.
5. **Require Software Bill of Materials (SBOM) with risk tracking** for critical software, coupled with **risk-based Plans of Action and Milestones** to close aged items.
6. **Institute a "People-Risk Program"** (to address threats like phishing or misconfigurations), with graduated consequences and role-based training, measured by advanced network analytics.
7. **Improve efficiency across multi-part supply chains by elevating information quality to downstream suppliers** with curated controls, templates, and onboarding support; incentivize primes to drive subcontractor performance.
8. **Adopt a Resilience Playbook with mission continuity metrics** (i.e., time-to-restore essential services) that is developed centrally, perhaps through OMB or GSA, and implemented across agencies along with recurring exercises.
9. **Leverage existing authorities** (such as contractual remedies or interim rules) to drive change, rather than waiting for long-cycle changes to the Federal Acquisition Regulations (FAR).
10. **Incorporate AI while minimizing related supply-chain risks through an AI Safety and Supply-Chain Charter for government**, again developed centrally (perhaps by NIST) and implemented in a risk-based fashion at the agency level. The charter could include principles for action, such as themes highlighted by participants:

> *Leadership buy-in is not enough, we need metrics and follow-through.*
>
> *Visible scorecards get attention at the highest levels.*
>
> *Reward outcomes, not effort—move security requirements left and measure results.*

In this roundtable, leaders from government, industry, and academia delved into how agencies can establish effective C-SCRM programs, the emerging threats they need to tackle, the role of automation, and the standards or KPIs that can help assess progress and ensure high ROI. This report highlights key insights from the session.

Government Cybersecurity—A Key Foundation for Supply Chain Risk Management

Adversaries—from criminal syndicates to nation-states—continue to target the federal supply chains, exploiting human error, legacy systems, opaque dependencies, and inconsistent enforcement. Early systems were primarily focused on perimeter security, firewalls, and intrusion detection. Over time, hackers have become more sophisticated, and cybersecurity systems have also had to improve and create additional layers of protection. Current cyber systems often include behavioral analytics and security event management, while agencies are also beginning to apply AI for threat detection and prevention; however, AI also presents risks, in the form of new attack vectors that can become available to hackers.

A federal supply chain cybersecurity system should reduce material risk to mission delivery from supply chain cyber threats. Success requires shortening the typical time required to detect and remediate vulnerabilities across enterprise and supplier ecosystems. This can be achieved by institutionalizing secure-by-design systems in procurement and vendor management, along with centralized cyber governance and resilience metrics (such as continuity metrics and recovery service level agreements (SLAs)) that are continuously tested. Unfortunately, many federal cyber initiatives are constrained by a number of factors, including budget ceilings, workforce gaps, legacy technology, long rulemaking cycles, decentralized missions, low risk appetites, and industry burden for compliance. These constraints may especially impact small vendors who serve as subcontractors or contributors at downstream supply chain tiers, starting with Tier 2 and Tier 3 suppliers.

Three Key Themes Discussed by Cyber Experts

Three themes consistently emerged from the discussion, discussed below.

Supply Chain Security and Acquisition

Participants found that, although many cyber policies exist, agencies can trade off security for performance under resource pressure. Centralizing critical cybersecurity responsibilities into a center of excellence, with decentralized implementation across agencies, can mitigate this risk. A lead Center could share information and common cyber services, even for a mission-specific environment.

> *In a constrained environment, Program Managers will trade off supply-chain security for other measures.*
>
> *Treat the Federal Government as an enterprise where we can share risk insights.*

An important element in such a governance system involves ensuring the right incentives and consequences. Vendors that outperform should receive positive rewards; chronic underperformers should face procurement consequences. Contracts can act as levers, and agencies should not have to wait for changes to the FAR. Contract terms and conditions (Ts & Cs) and cooperative purchasing vehicles can embed requirements and enforce these terms. Complementing contracts with scorecards, either public or executive, can attract leadership attention and drive behavior.

> *Why keep buying from vendors with major incidents?*
>
> *Contracts are the lever—enforce them.*

AI, Automation, and Data

A second theme involves automation and data. The public and private sectors are moving towards a machine-oriented future, and AI is already enabling vulnerability discovery, triage, and remediation options**.** Human error remains a primary source of vulnerability, often through social engineering hacks. Misconfigurations and phishing are still leading vectors of attack in most intrusions. Recent research[1] shows that 70 percent of breach notices in the first half of 2025 did not specify the attack vector, reflecting gaps in visibility and attribution. This lack of transparency impedes response efforts. AI-driven analytics that fuse signals from multiple data sources can help close these visibility gaps and provide more precise attribution.

> *AI-backed analytics should target real-time consequences.*

Data quality remains critical to ensure that supply chains operate with accurate information. Actions must be taken to reduce the possibility of data entry error, as well as data manipulation. Agencies can continuously check on data correctness and the possibility of its manipulation by hackers, who can enter a database and make alterations that interfere with business processes. Continuous monitoring practices can help agencies to check for anomalies, integrity issues, and other indicators of data drift. Even in highly secure environments, simple human errors or system inconsistencies can disrupt operations, making ongoing validation essential.

Equally important is the ability to integrate and correlate data from multiple internal and external sources. Bringing these data sets together creates a more comprehensive, enterprise-level view of supply chain posture, enabling organizations to better anticipate risks, orchestrate mitigation activities, and make informed decisions. By unifying data streams across systems, stakeholders gain greater visibility and can more effectively coordinate actions to prevent, detect, and respond to cyber supply chain risks.

AI capabilities can further strengthen these C-SCRM activities by accelerating anomaly detection, synthesizing insights across vast data sets, and supporting proactive risk mitigation. Moreover, strong governance, transparency, and provenance controls will ensure the AI itself is secure, trustworthy, and aligned with organizational standards.

Governance, Resilience, and Future State

Under a third theme, federal agencies need to define success in terms of continuity. Many resources can operate together to enable resilient future supply chains, including the Federal Acquisition Security Council (FASC) and CIO Council mechanisms aligned with policies and practices from OMB, ONCD, NIST, and DHS/CISA.

Along with aligned governance, development of performance metrics is critical, as is ensuring that all parties have access to common dashboards. Aligned with having “outcome-based governance,” metrics should track “outcomes over outputs.” An important set of scorecard design principles for supplier cybersecurity begins with clear definitions, a small set of leading indicators, automated collection of metrics, regular executive drill-downs to understand deficiencies, review of trend lines, and transparent thresholds for incentives and consequences.

[1] Verizon 2025 Data Breach Investigations Report

As one executive noted, metrics ensure that program managers pay attention to outcomes. Some of the most common metrics include:

- **Mission recovery objectives:** Time-to-Maintain-Minimum-Service (TMMS) ≤ 4h; Time-to-Full-Service (TFS) ≤ 48h for essential systems.
- **Exercise cadence:** Quarterly for crown jewels; semi-annual for supporting systems.
- **Risk burn-down:** # critical vulnerabilities >30/60/90 days; % exploitable vulnerabilities mitigated; supplier incident recurrence rate.
- **Continuity:** Time to restore essential services; # successful resilience exercises; dependency health index.
- **People risk:** Phish-fail rate (by role); privileged error rate; MFA/least-privilege coverage.
- **Supplier performance:** Tier status; sub-tier coverage; T&C addendum acceptance; SBOM + telemetry completeness.
- **Automation impact:** SOC triage time; patch MTTR; % automated remediations within guardrails; false-positive rate.

> *How quickly can essential services resume under cyber disruption? Bake into KPI and SLAs.*
>
> *Sustain momentum with recurring executive reviews and mission-owner engagement.*

Given the prominence of cybersecurity as an element in corporate risk, companies are quickly beginning to make investments in cybersecurity that span more than one business function. Budgeting for cybersecurity in supply chain management function is also essential. But while cyber threats continue to grow, spending on cybersecurity isn’t necessarily keeping up. Multiple studies show that at the median, organizations only spend half of one percent of their total revenue on cybersecurity.

Strategic Initiatives

The roundtable discussion pointed to several potential options that could be implemented by government. Box B at the end of this section suggests a model action plan.

Initiative A—Enterprise C-SCRM CoE and Executive Dashboard

GSA or another lead agency could stand up an enterprise C-SCRM CoE and Dashboard. This Center could coordinate actions outlined below, working with OMB.

Objective: Create a shared service that consolidates risk intake, analytics, supplier performance, and remediation orchestration across agencies.

Potential Scope: Vendor risk registry, incident intake, Software Bill of Material (SBOM) and real-time telemetry system monitoring critical supply chain systems. Develop tiered supplier merit scores for Tier 1, 2, and 3 suppliers, ensure contractual T&C compliance status, and product ID mappings to contracts. Supplier performance feeds delivered into the CoE and rolled up into an executive dashboard.

Initiative B—Secure-by-Design Vendor Merit Program

Create a Secure-by-Design Vendor Merit Program with tiered incentives and consequence pathways for repeat incidents.

- **Objective:** Shift market behavior with carrots and sticks for critical suppliers.
- **Potential Scope:**
  - **Tiers:** Platinum/Gold/Silver based on verified controls, incident history, response performance, and third-party posture.
  - **Incentives:** Faster awards, evaluation credits, reduced evidence friction for top tiers.
  - **Consequences:** Mandate annual security addenda for multi-year MSAs to keep obligations current; track acknowledgments digitally and enforce via contract remedies. Conditional awards, corrective action plans, or exclusion from critical workloads for repeat failures.

Initiative C—AI-Driven Continuous Diagnostics & Remediation (CDR)

- **Objective:** Ensure Mean Time to Discovery/Mean Time to Recovery metrics are reviewed by senior executives regularly, and rely on automation and intelligent triage.
- **Potential Scope:** Capabilities to require SBOM plus runtime telemetry for critical software; tie to risk-based remediation SLAs, transparent reporting, and agent-based patching; LLM copilots for analysts; policy-constrained autonomous actions for low-risk classes. Consolidate overlapping tools into a platform architecture that reduces complexity, but retain third-party telemetry to avoid single-vendor blind spots

Initiative D—Institutionalize People-Risk Reduction Programs That Drive Culture Change

- **Objective:** Reduce people-driven risk by increasing automation within C-SCRM workflows. Automating routine checks, data validation steps, and configuration reviews helps minimize human error and accelerates risk detection. Humans remain essential, but their role shifts to validating and adjudicating automated findings rather than performing end-to-end manual execution—improving efficiency, scalability, and overall resilience. This can also reduce social engineering incidents and misconfigurations.
- **Potential Scope:** Implement adaptive phishing training programs, role-based hands-on labs, and targeted instruction supported by advanced analytics to identify susceptibility to phishing and common configuration errors. Graduated consequences can be used to incentivize positive behaviors and discourage negligence. For example, repeated training failures could trigger additional coaching, more intensive training, and ultimately HR action if necessary; while suppliers who show reduction in critical risk metrics, provide and maintain accurate SBOMs, and engage proactively with the government to reduce cyber supply chain risk could be rewarded by contract incentives. Such incentives could be based on metrics that include: (See Box A for additional risk factors and mitigations)
  - **Risk burn-down:** Number of critical vulnerabilities after 30/60/90 days; percent of exploitable vulnerabilities mitigated; supplier incident recurrence rate.
  - **Continuity:** Time to restore essential services; # successful resilience exercises; dependency health index.
  - **People risk:** Phish-fail rate (by role), privileged error rate, MFA/least-privilege coverage.
  - **Supplier performance:** Tier status; sub-tier coverage; T&C addendum acceptance; SBOM + telemetry completeness.
  - **Automation impact:** Triage time; patch MTTR; percent automated remediations within guardrails; false-positive rate.

> *Visible public scorecards get presidential and secretary attention.*
>
> *Reward outcomes—not effort.*
>
> *AI can map the entire supply chain down to package level and surface where risks intersect.*
>
> *Human errors are the scariest; focus on what people actually do.*

Box A—Risk Registry and Mitigations

Risk	Likelihood	Impact	Mitigation
Vendor resistance to merit tiers/consequences	Medium	High	Early RFI/comment period; clear criteria; phased enforcement; appeal path.
Data quality/integration delays	High	Medium	Start with top vendors & crown jewels; normalize IDs; create a master data dictionary; automate ingestion.
AI model/guardrail failure	Medium	High	Model attestations, red-teaming, human-in-the-loop for high-risk actions, rollback plans.
SMB burden (Tier-2/3)	Medium	Medium	Uplift program with templates, tooling, and prime-sponsored support; scaled evidence.
Legal/PR concerns with scorecards	Medium	Medium	Limit initial metrics; counsel review; focus on trends and remediation, not blame.
Cultural pushback on consequences	Medium	High	Executive sponsorship; clear linkage to mission risk; celebrate wins publicly.

Initiative E—Improve Cross-Tier Supplier Uplift and Onboarding

- **Objective:** Expand secure capacity without excluding small and medium-sized business (SMBs).
- **Potential Scope:** Standard control kits, template plans, subsidized scanning, helpdesk, and prime-led mentoring. Contractual changes include flow-down clauses; regular attestation cadence; corrective action timelines; capability credits for primes that uplift subs.

> *Let's make it **easier for suppliers** to get onboard securely.*
>
> *Define success by **how quickly essential services recover**.*

Initiative F—Policy and Contracting Recommendations

- **Objective:** Align policies to drive consistent actions that improve cybersecurity for supply chain risk management.
- **Potential Scope:**
  - **Use existing authorities**: Invoke FASC, OMB, and FAR Council referrals and agency-level remedies for persistent, material security failures—agencies should not wait for final FAR rules.
  - **Embed annual security addenda** in long-term contracts and service agreements to keep pace with threat evolution.
  - **Evaluation credits** in source selections for secure-by-design performance (incident handling, SBOM completeness, Tier 2/3 enforcement).
  - **Standard clause library** for C-SCRM (flow-downs, telemetry, incident reporting within 24 hours, exploitability-based patch SLAs).
  - **Interagency data-sharing MOUs** to support the CoE and reduce duplicative burden on industry (single evidence submission, multi-agency use).
  - **POA&M modernization**: risk-weighted closure SLAs; enforce aged critical items; tie to vendor merit status.

Box B—Model Action Plan

Day 0–30 (Mobilize & Baseline)

Appoint Executive Sponsor and CoE Lead.

- *Owners:* Agency CIO/CISO + Acquisition Executives.
- *Milestones:* Charter, RACI, backlog list, sponsor letter, steering committee.

Stand up an initial C-SCRM dashboard (MVP) pulling top 50 vendors, open critical vulnerabilities, POA&M aging, and phishing metrics.

- *Owners:* CoE + Security Ops Center + Procurement Data Leads.
- *Milestones:* Live dashboard with weekly refresh.

Issue security T&C addendum template for all MSAs and active contracts.

- *Owners:* Chief Procurement Officer (CPO), General Counsel.
- *Milestones:* Template approved, distribution plan.

Publish Vendor Merit Program draft criteria and request for comment to supplier community.

- *Owners:* CoE + CPO.
- *Milestones:* Criteria posted, comment window open.

Launch People-Risk quick win, adaptive phishing campaign + role-based micro-training.

- *Owners:* CISO + HR.
- *Milestones:* Baseline phish-fail rate captured.

Day 31–60 (Build & Pilot)

Integrate SBOM & runtime telemetry for top critical applications; start exploitability scoring.

- *Owners:* Application Security + SOC.
- *Milestones:* SBOM coverage ≥70% of crown-jewel systems.

Pilot AI-assisted Tier-1 SOC triage and **automated patch orchestration** for low-risk classes.

- *Owners:* SOC + Platform Ops teams.
- *Milestones:* 25% reduction in mean ticket handling time.

Execute Tier-2/3 Supplier Uplift cohort #1 (20 suppliers).

- *Owners:* Primes + CoE supplier enablement.
- *Milestones:* 80% complete baseline controls, corrective action plans for rest.

Run Resilience Exercise #1 on one essential service; capture TTR baseline.

- *Owners:* Mission + Continuity Office.
- *Milestones:* After-action report, top 5 remediation items.

Day 61–90 (Scale & Enforce)

Publish initial Vendor Merit tiers; align **evaluation credits** for new awards; notify vendors requiring corrective actions.

- *Owners:* CPO + CoE.
- *Milestones:* Tier list published, incentives active in solicitations.

Turn on consequence management for aged high-risk POA&Ms (>90 days).

- *Owners:* CIO/CISO + CPO.
- *Milestones:* 50% reduction in aged critical POA&Ms.

Expand CDR coverage (assets, apps, network sensors); formalize AI guardrails (model attestations, data handling).

- *Owners:* CISO + Data Gov.
- *Milestones:* Guardrails signed, coverage >60% of prioritized estate.

Publish public scorecard pilot (limited metrics).

- *Owners:* CoE + Comms + OGC.
- *Milestones:* Web page live, quarterly cadence established.

Year 1–2

Q1: Stand up CoE, dashboard MVP, people-risk program, T&C addenda rollout; AI triage pilot.

Q2: Publish vendor merit tiers; expand telemetry; resilience exercises across top 3 essential services.

Q3: Scale Tier-2/3 uplift; public scorecard metrics; automate patch orchestration for medium-risk classes.

Q4: Cross-agency data-sharing MOUs; broaden incentives; independent assessment of outcomes; refresh roadmap.

Conclusion

Roundtable participants highlighted the complexity of securing digital infrastructure in a dynamic threat environment. Key findings include:

- **Establish clear metrics and accountability mechanisms** through Centers of Excellence and public reporting.
- **Adopt secure-by-design principles** as standard practice for both government and industry vendors.
- **Leverage AI and automation** to enhance proactive defenses while maintaining human oversight.
- **Support resilience** by defining outcome-based metrics and ensuring continuous diagnostics.
- **Expand support for small and medium businesses** to enable secure participation in federal supply chains.
- **Engage Congress and policy makers** to ensure sustainability and scalability of reforms.
- **Foster a cybersecurity-first culture** across agencies and industries, with robust training and awareness programs.

As one participant summarized, *“Culture must infuse the will to do it because of the mission, impact, and benefit.”* This cultural transformation, combined with governance reform and technological innovation, is essential to safeguarding the nation’s digital infrastructure.

About the Author

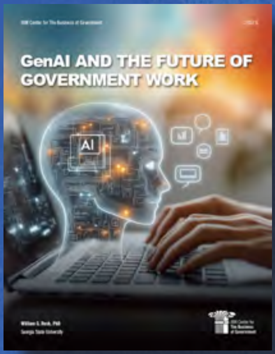
Dr. Robert Handfield
Bank of America University Distinguished Professor of
Supply Chain Management
North Carolina State University
Department of Business Management
College of Management
Raleigh, North Carolina 27695

P: 919 515-4674
E: robert_handfield@ncsu.edu

Dr. Rob Handfield is the Bank of America University Distinguished Professor of Supply Chain Management at North Carolina State University, and Executive Director of the Supply Chain Resource Cooperative (http://scm.ncsu.edu/). Handfield is considered a thought leader in the field of supply chain management, and is an industry expert in the field of strategic sourcing, supply market intelligence, and supplier development. He has spoken on these subjects across the globe, including China, Azerbaijan, Turkey, Latin America, India, Europe, Korea, Japan, Canada, in multiple presentations and webinars.

Dr. Handfield has published more than 120 peer-reviewed journal articles and is regularly quoted in global news media such as the *New York Times, Wall Street Journal, LA Times, Bloomberg, NPR, Washington Post, the Financial Times, the San Francisco Chronicle*, and CNN. He served on the Joint Acquisition Task Force during COVID which led to published articles on the shortages of PPE in the *Harvard Business Review* and the *Milbank Quarterly Journal,* and led a NIIMBL research team studying distribution of test kits during the pandemic. He was also invited to serve on the Biden White House Council of Economic Advisors in January 2022, and has worked with many companies through the Supply Chain Resource Cooperative for several years.

Recent Reports from the IBM Center for The Business of Government



GenAI and the Future of Government Work

by William G. Resh

Embedding Strategic Foresight into Strategic Planning and Management

by Bert George

Collaborative Public Engagement for Building Trust in Government

Resilience in action: Crisis leadership through innovation, collaboration, and human-centered solutions

by Julia Carboni

RESPONSIBLE AI FOR PUBLIC EVALUATION
Harnessing AI to Strengthen Public Sector Decisions

Responsible AI for Public Evaluation

by Daniel Fonner

SPECIAL REPORT
FIVE PILLARS OF EFFECTIVE GOVERNMENT
PARTNERSHIP
WORKFORCE
EFFECTIVENESS
DATA
TECHNOLOGY
Daniel J. Chenok • Margie Graves • Michael J. Keegan

Five Pillars of Effective Government

by Dan Chenok

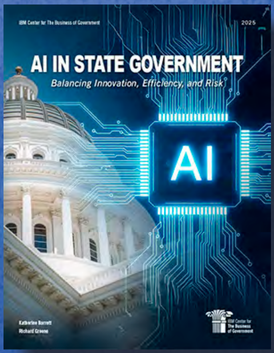
Government's Digital DNA: Identity and Access Management for Public Sector Security

by Andrew Whitford

Building community-based resilience
Emergency preparedness and response case studies
IBM

Building community- based resilience

by Authors of Case Study



AI in State Government

by Katherine Barrett and Richard Greene

For a full listing of our reports, visit businessofgovernment.org/reports

About the IBM Center for The Business of Government

Through research stipends and events, the IBM Center for The Business of Government stimulates research and facilitates discussion of new approaches to improving the effectiveness of government at the federal, state, local, and international levels.

About IBM Consulting

With consultants and professional staff in more than 160 countries globally, IBM Consulting is the world's largest consulting services organization. IBM Consulting provides clients with business process and industry expertise, a deep understanding of technology solutions that address specific industry issues, and the ability to design, build, and run those solutions in a way that delivers bottom-line value. To learn more visit ibm.com.

For more information:
Daniel J. Chenok
Executive Director
IBM Center for The Business of Government

600 14th Street NW
Second Floor
Washington, D.C. 20005
(202) 551-9342

website: www.businessofgovernment.org
e-mail: businessofgovernment@us.ibm.com

IBM Center for
The Business
of Government