GovExec

Friday, March 27, 2026

7:30 AM EDT
1 HR

Registration, Breakfast & Networking

Pick up your badge and enjoy networking with your peers!

8:30 AM EDT
5 MINS

Welcome & Introduction

Nick Wakeman
Editor-in-Chief
Washington Technology

Washington Technology will kick off day by introducing our 1st speaker and setting the stage for today's discussions.

8:35 AM EDT
20 MINS

Securing the Arsenal: A Conversation on the Defense Industrial Base

Mike Derrios
Executive Director, George Mason University's Baroni Center for Government Contracting
GMU

Nick Wakeman
Editor-in-Chief
Washington Technology

The defense industrial base is under pressure from every direction—cyber threats, supply chain vulnerabilities, workforce shortages, and a procurement system struggling to keep pace with modern threats. How resilient is the DIB, and what will it take to strengthen it? This Q&A with Mike Derrios, Director of the Greg and Camille Baroni Center for Government Contracting at George Mason University, will take stock of the industrial base that underpins U.S. national security. From the most pressing cybersecurity risks to the talent pipeline challenges that could shape the DIB's long-term capacity, Derrios will offer a practitioner's perspective on where the gaps are and who needs to close them.

8:55 AM EDT
15 MINS

CMMC's Hidden Risks: What a New GAO Report Reveals

Joseph Kirschbaum
Director, Defense Capabilities and Management
GAO

Nick Wakeman
Editor-in-Chief
Washington Technology

The Pentagon's cybersecurity certification program for defense contractors is entering a critical implementation phase, and a new government watchdog report says the Department of Defense needs to do more to prepare for the obstacles ahead. Join us for an exclusive conversation with one of the authors of a newly released GAO report on the Cybersecurity Maturity Model Certification (CMMC) program, which found that while DoD's rollout plans are largely on track, the department has yet to fully account for key external risks. Our guest will walk through the findings and what they mean for contractors navigating CMMC compliance.

9:10 AM EDT
15 MINS

Your CMMC Assessment Follows Your Data, Not Your Org Chart

Tom Tapley
Manager, Federal Programs
Sonatype

CMMC assessment scope follows the data — not the org chart — meaning that Controlled Unclassified Information (CUI) drives what must be protected and assessed, regardless of where it resides or through whom it flows. As CMMC implementation timelines tighten and agencies and contractors wrestle with SBOM expectations and zero-trust mandates, unmanaged vendor risk is emerging as a key finding in third-party assessments and a source-selection differentiator.

In this session, we unpack how assessors and acquisition stakeholders are shifting from a checklist mindset to real-world risk evaluation by probing three failure points across the software supply chain:
Prevent — ensuring intake controls actually stop vulnerable and malicious components before they enter build pipelines, beyond NVD-only blocking;
Govern — documenting and bounding policy exceptions with compensating controls, especially for end-of-life and high-risk components;
Prove — demonstrating compliance as a living signal through continuous monitoring, impact analysis, and reproducible artifacts like SBOMs.
We close with concrete flow-down expectations for primes and vendors alike — including intake controls, exception management discipline, and continuously updated component inventories — and show why visibility into both prime and vendor software supply chains is the essential first step to surviving CMMC assessments. With enforcement tightening, continuous verification of vendor security isn't optional — it's a competitive advantage.

9:25 AM EDT
30 MINS

Certification Transition: Navigating ISACA's New Role in CMMC Assessments

Todd Gagnon
Director, CMMC Assessor and Instructor Certification Organization (CAICO)
ISACA

Nick Wakeman
Editor-in-Chief
Washington Technology

With ISACA now managing CMMC assessor certifications, contractors and assessors alike are adapting to a new landscape. During this session, Todd Gagnon from ISACA will examine how assessor credentialing, training pathways, and quality assurance processes are evolving, and what those changes mean for contractors planning for certification. This session will also address assessor capacity, market readiness, and practical steps organizations can take to position themselves for successful assessments amid growing demand.

9:55 AM EDT

30 MINS

Operationalizing CMMC: Lessons from Early Implementers

Tom Terjeson
Chief Information Officer
Peraton

JR Williamson
CISO
Leidos

Nick Wakeman
Editor-in-Chief
Washington Technology

Protecting the defense industrial base depends on more than policy; it requires organizations to implement CMMC across every level of operations. This session will feature practitioners and industry leaders sharing real-world lessons from early implementation efforts, including scoping and boundary definition, control prioritization, tooling versus process decisions, and managing cost and timeline expectations. Speakers will discuss common pitfalls, proven approaches, and how organizations can build sustainable cybersecurity programs that strengthen security posture while supporting mission delivery.

10:25 AM EDT

5 MINS

Closing Remarks

Nick Wakeman
Editor-in-Chief
Washington Technology