NDIA

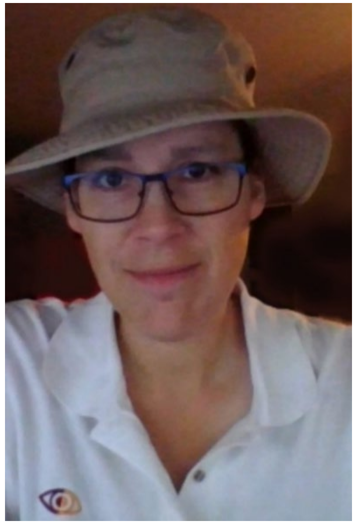
CMMC: Update, 3rd Party Assessor Requirements & Zero Trust

Current As Of: April 2023

Sponsored by:
COALFIRE® FEDERAL

TODAY'S SPEAKERS

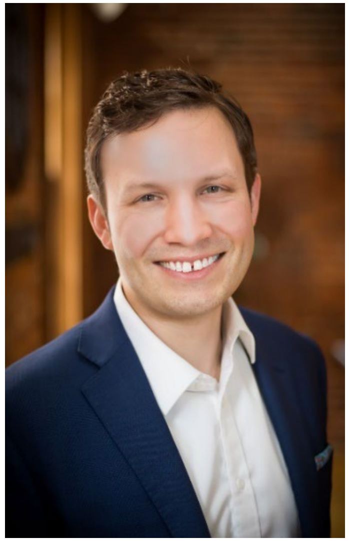
NDIA



Amira Armond

President

Kieri Solutions
Vice Chair, C3PAO Stakeholder Forum



Ryan Heidorn

Chief Technology Officer

C3 Integrated Solutions
Board Director, NDIA New England

Vince Scott

CEO

Defense Cybersecurity Group
INFRAGARD National SME Cyberwarfare

Sponsored by:
COALFIRE FEDERAL

7th Annual Cyber Event

MAY 10, 2023

Gillette Stadium, Foxboro MA

NDIA New England

Protecting our Advantage: CMMC, Cybersecurity Compliance, and Resilience

COL Candice E. Frost
U.S. Army
Former JIOC Commander,
USCYBERCOM

The Hon. Jim Langevin
Former Chairman,
House Armed Services Subcommittee
on Cyber, Information Technologies
and Innovation

Dr. David Mussington
Executive Assistant Director for
Infrastructure Security, CISA

Kristen M. Lane
Senior Intelligence Analyst,
FBI

The Hon. David L. Norquist
President and CEO, NDIA

Full agenda online: ndianewengland.org

Save $25 off registration with promo code: CMMCuthere

Expires Friday, April 21

Protecting our Advantage: CMMC, Cybersecurity Compliance, and Resilience

NDIA

Tales from the Trenches: What to Expect from a CMMC/NIST SP 800-171 Assessment

Nick DeLena
Partner, Cybersecurity and Privacy Advisory, PKF O'Connor Davies

Matthew Travis
CEO, The Cyber AB

Scott Whitehouse
Practice Lead, Security and Compliance, C3 Integrated Solutions

Deborah Hunt
CEO, iPower

Charles Connolly
Group Chief, Business Operations, DIBCAC, DCMA

Cybersecurity: The Harsh Criminal, Civil, and Administrative Penalties of Non-Compliance

Robert Metzger
Head of Washington Office, Chairman of Cybersecurity and Privacy Practice Group Rogers Joseph O'Donnell, PC

B. Stephanie Siegmann
Chair Cybersecurity, Privacy & Data Protection Group; Litigation Partner, Hinckley Allen; Former National Security Chief (U.S. Attorney's Office/D. Mass.)

Full agenda online: ndianewengland.org

Save $25 off registration with promo code: CMMCuthere

Expires Friday, April 21

Secure Your Networks and Systems In Physical Space and Cyberspace

- **Secure your Networks. Now**
- DFARS 7012 / NIST 800-171 impose current Contractual Obligations
- Self-Assessment did not incentivize companies to comply
  - Does not negate obligation to meet the Standards in the Cybersecurity Framework

Secure Your Networks and Systems In Physical Space and Cyberspace

- **Be prepared for uncertainty**
  - Follow your contractual requirements
  - Meet all existing cybersecurity obligations
    - FCI vs. CUI vs. CDI
  - Remain "current, accurate, and complete"
  - Government's lack of clarity is dangerous
    - Communicate effectively – to all
  - Educate your customers (Federal & Prime)
- **Enforcement and Oversight**
  - What mechanisms/tools outside of NIST/CMMC can/will the government use to ensure compliance?
    - Prime contractor arm-pulling?
    - Hold back?
    - False Claims Act?
    - Specialized clauses - NMCARS 5204.73
      - "material requirement"

Sponsored by:

COALFIRE FEDERAL

May Webinar: Everything you want to know about Compliance!

- Focus on Compliance overall, not simply CMMC
- As some companies achieve compliance, concern costs make them non-competitive
- Is DoD incentivizing companies to delay?

Sponsored by:

COALFIRE FEDERAL

New National Cybersecurity Strategy

- **2 Fundamental Shifts:**
  - Rebalance responsibility to defend cyberspace
  - Realign incentives to favor long-term investments
- **Digital ecosystem’s biggest, most capable, and best-positioned actors CAN and SHOULD assume greater share of the burden for mitigating cyber risk**
  - Public or Private sectors
  - Trade-off between temporary fixes and long-term solutions
  - Ensure resources, capabilities, incentives to choose long-term
- **“What” and “How”**
  - Requires true partnership

Update

- **CMMC proposed rule**
- **7024 issued as a final rule**
  - Directs contracting officers to consider supplier risk during evaluation process
- **Anticipated early April update**
  - Will provide KOs with guidance about using SPRS to determine supply chain risk
  - Possible DoD updates guidance to include consideration of Cybersecurity risk
- **SPRS must be accurate**
  - Anecdotal evidence indicates most companies believe they are more secure than they are

Requirements to be 3rd Party Assessor

CMMC Professional (minimal participation in assessment)	CMMC Assessor (full participation)
US Citizen + Government Background Investigation	CMMC Professional requirements
2+ years experience or degree in IT / cyber	+Formal training (5 day)
Formal training (3-5 day)	+Exam
Pass exam	+ 3 assessments as a Professional

Lead Assessor
TBD (likely another formal training)

Sponsored by:

3rd Party Assessment Organization

NDIA

Assessment Capabilities

- Assessor training and experience
- Assessor background checks
- Conflict of Interest review
- Planning
- Logistics
- Assessment
- Reporting
- Appeal handling

Secure Information System

- Pass CMMC Level 2
- Protect client information
- Interface with Gov Database

Quality Management

- Quality Program
- Complaint handling
- Organizational background checks

Sponsored by:

COALFIRE FEDERAL

3rd Party Assessor – Implied Responsibility

- **Want to see clients succeed**
  - Problem: most companies underestimate effort needed to pass
  - Reviews to avoid assessing unprepared companies
- **Flexible methods, inflexible results**
  - 198 out of 320 requirements are pass/fail for the entire assessment
- **Some concepts very complex and follow IT best practices:**
  - Risk assessment, change management, vulnerability management

Zero Trust

- **Assume your network is compromised**
  - *"Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems."* **SC.L2-3.13.2**
- **Implications for CMMC / NIST SP 800-171**
  - *Importance of scoping, especially for cloud-based systems*
- **Tactical guidance in OMB Memo M-22-09**
- **DoD Zero Trust Strategy**
  - *"[R]epresents a major cultural change that stakeholders throughout…the Defense Industrial Base, will need to embrace and execute beginning with FY2023…" (link)*

NDIA Recommendations

- **Current plan as NDIA understands it will result in significant failure rates across the DIB (and government)**
- **3 Recommendations**

1. **IAW new Cybersecurity Strategy, DoD CIO include industry in their assessment plan**
   – NDIA recommends focusing on “How” and “What”
2. **“How” – Adjust implementation plan**
   – Assess MSPs as part of a cohesive strategy; verify providers meet standards on behalf of their clients
   – Identify controls assessors can identify for immediate correction
   – Limit controls that drive automatic fail
3. **“What” – Limit scope of material for protection**
   – Require senior leader approval

Sponsored by:

Secure Your Networks and Systems In Physical Space and Cyberspace

- **Be working on these controls now!**
  - 18-24 months a reasonable, serious timeline; lower costs
  - 7 months a crash program with heavy investment
  - 7 days / 7 weeks un-executable at any cost
- Prioritize!
  - Some controls provide larger impact
  - 100% implementation extremely difficult

NDIA

7th Annual Cyber Event

MAY 10, 2023

Gillette Stadium, Foxboro MA

Protecting our Advantage: CMMC, Cybersecurity Compliance, and Resilience

COL Candice E. Frost
U.S. Army
Former JIOC Commander,
USCYBERCOM

The Hon. Jim Langevin
Former Chairman,
House Armed Services Subcommittee
on Cyber, Information Technologies
and Innovation

Dr. David Mussington
Executive Assistant Director for
Infrastructure Security, CISA

Kristen M. Lane
Senior Intelligence Analyst,
FBI

The Hon. David L. Norquist
President and CEO, NDIA

Full agenda online: ndianewengland.org

Save $25 off registration with promo code: CMMCuthere

Expires Friday, April 21

Questions?

Sponsored by: