CMMC Update:
Notice of Proposed Rulemaking
NDIA Comments

Current As Of: February 2024

TODAY'S SPEAKERS

Amira Armond
President
Kieri Solutions
Vice Chair, C3PAO Stakeholder Forum

Ryan Heidorn
Chief Technology Officer
C3 Integrated Solutions
Board Director, NDIA New England

A.R. "Trey" Hodgkins, III
CEO and President
Hodgkins, Consulting LLC
Chair, NDIA Cybersecurity Division

Vince Scott
CEO
Defense Cybersecurity Group
INFRAGARD National SME Cyberwarfare

Sponsored by:

abacode
Cybersecurity & Compliance

Secure Your Networks and Systems In Physical Space and Cyberspace

- Secure your Networks. Now
- Contractual obligation to comply with National Institute of Standards and Technology (NIST) 800-171Rev2
  - Companies not complying sufficiently under current regulation
  - Does not negate obligation to meet the contractual requirements
- CMMC announced Jul ’19 -- 3rd Party Assessments to ensure 800-171 implementation in the future
  - CMMC 2.0 announced Nov ’21
- DRAFT NIST 800-171Rev3 released 10 May 23
  - Final draft out for comment – Closed January 26th
- CMMC NoPR released 26 Dec 23

Sponsored by:

abacode Cybersecurity & Compliance

NDIA Regulatory Comment Development Process

- NDIA Strategy & Policy Team
  - Strategic partner to 27 Divisions
  - Coordinates regulatory comments
    - Drafting within Division membership
    - Receive and compile member inputs
    - Consensus: Deconflict with other Divisions
    - Finalize with Division Leadership
    - Submit Filing
  - Additional policy actions outside comments
- Cybersecurity Division, Chair
  - Trey Hodgkins (CEO, Hodgkins Consulting, LLC)
    - Bio & Introduction

NDIA Cybersecurity Division: CMMC Comments

- **Controlled Unclassified Information (CUI)**
  - **Critical to risk management goals of CMMC**
  - **Delineate clear and actionable marking instructions**
  - **Harmonize across Federal Government**
  - **Formalized process with industry to establish clear and consistent CUI marking guidance**

NDIA Cybersecurity Division: CMMC Comments

- CMMC 2.0 increases cost and scope beyond contractual requirements
  - Cost not simply determined by number of security requirements
  - Requirements placed on larger number of systems and organizations outside principal organization
    - Increased scope = increased costs
  - Rule will increase the cost of serving government customers across the DoD

NDIA Cybersecurity Division: CMMC Comments

- Transition between NIST SP 800-171 Rev2 and Rev3
  - Phased approach with clear deadlines
  - Consider class deviation
- Plan of Action and Milestones (POA&Ms)
  - Large number controls simply pass/fail
  - Small businesses may need more than 180 days
  - Allow failed objectives to be re-assessed without new full assessment
  - Assessment costs are allowable…including reassessments

NDIA Cybersecurity Division: CMMC Comments

- Narrow scope of CSP and define additional terms
  - Cloud Service Provider (CSP) – Broad Definition
    - CSP/Other than CSP not clear – No mechanism to determine
    - Align CSP to definition of Cloud Services in NIST 800-145
    - Reference definitions of CSP/MSP in Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA)
  - Security Protection Data (SPD) – Not Defined
  - Customer Responsibility Matrix (CRM) for ESPs

Secure Your Networks and Systems In Physical Space and Cyberspace

- **Secure your Networks. Now**
- **Contractual obligation to comply with National Institute of Standards and Technology (NIST) 800-171Rev2**
  - **Companies not complying sufficiently under current regulation**
  - **Does not negate obligation to meet the contractual requirements**
- **Communicate with your MSPs/MSSPs/ESPs**
  - **Be ready for implementation of the final rule**

Questions?

Sponsored by:

abacode
Cybersecurity & Compliance