CMMC:
Assessment Preparation
&
Sustaining Excellence

Current As Of: 15 March 2023

NDIA New England Chapter 7th Annual Cyber Event

Protecting our Advantage:

CMMC, Cybersecurity Compliance, and Resilience

10 May 2023

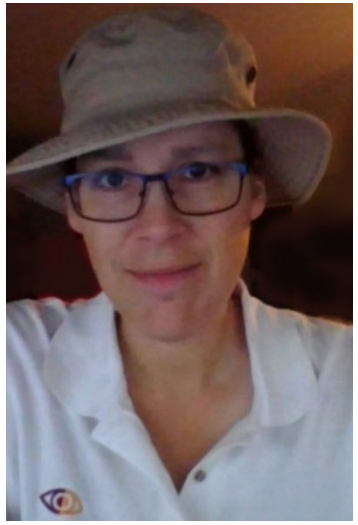
Gillette Stadium, Foxborough, MA

For more information visit: ndianewengland.org

Sponsored by:

COALFIRE FEDERAL

TODAY'S SPEAKERS



Amira Armond

President

Kieri Solutions
Vice Chair, C3PAO Stakeholder Forum

Alex Major

Attorney

McCarter and English

Vince Scott

CEO

Defense Cybersecurity Group
INFRAGARD National SME Cyberwarfare

Sponsored by:

COALFIRE FEDERAL

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

Sponsored by:

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”

NDIA Concerns – Information Protection

- We cannot protect 100% of our **UNCLASSIFIED** information/data 100% of the time with 100% perfect controls implementation
- Business must understand the scope and scale of the requirement to effectively build their IT infrastructure and processes
- Government personnel must:
  - Understand protection requirements
  - Understand what information requires protection
  - Accurately mark information requiring protection
  - **"CUI is CUI" is not the answer – Government must provide contractors with clear guidance on the narrowly defined data they must protect**
- CIO is working on a guidebook for contracting officers
  - Interpretation will likely drive differing implementation
  - Possible different KOs will impose different requirements on a single business (Army vs Navy vs AF contracts)

What do companies need to protect?

- **Protection is required of a vast array of data**
  - Should:
    - Banking information
    - Intellectual Property (IP)
    - Supply chain sources and methods (*see, e.g.,* business email compromise)
    - IT infrastructure buildout
  - Must:
    - HR Information (PII/PHI, etc.)
    - Classified information
    - Federal Contract Information
    - Controlled Unclassified Information (CUI)

Defining Controlled Unclassified Information (CUI)

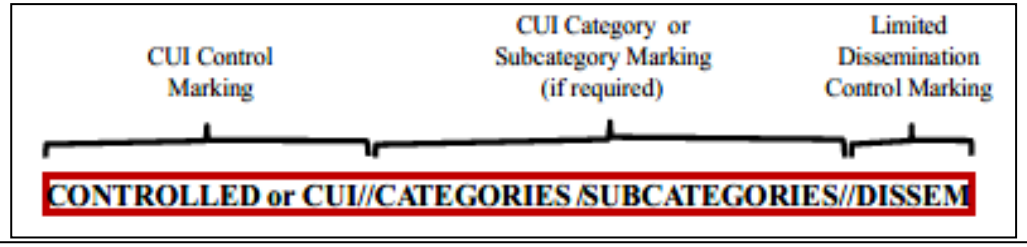
- **Federal Contract Information (FCI)**[1] – CMMC 2.0 Level 1
  - "FCI is information not intended for public release. FCI is provided by or generated for the Federal Government under a contract to develop or deliver a product or service."
- **Controlled Unclassified Information (CUI)**[1] – CMMC 2.0 Levels 2-3
  - "CUI and FCI share important similarities and a particularly important distinction. Both CUI and FCI include information created or collected by or for the Government, as well as information received from the Government. However, while FCI is any information that is "not intended for public release," CUI is information that requires safeguarding and may also be subject to dissemination controls. In short: **All CUI in possession of a Government contractor is FCI, but not all FCI is CUI."**

Defining CUI – A Continuing Challenge

- "CUI and FCI share important similarities and a particularly important distinction. Both CUI and FCI include **information created or collected by or for the Government**, as well as information **received from the Government**. However, while FCI is any information that is "not intended for public release," CUI is information that **requires safeguarding and may also be subject to dissemination controls**. In short: All CUI in possession of a Government contractor is FCI, but not all FCI is CUI."

Controlled Unclassified Information (CUI)

- **A broad category of information that a law, regulation, or government-wide policy requires agencies and contractors to handle using dedicated safeguards or dissemination controls**
- **Examples of CUI include, but are not limited to:**
  - Procurement and acquisition information (e.g., source selection data)
  - Proprietary business information
  - Critical infrastructure information (e.g., U.S. energy infrastructure)
  - USG survey and statistical information
  - Defense information (e.g., controlled technical information)
  - Export control information



CUI//CENS

CONTROLLED//SP-CTI//NOFORN

CUI//SP-PROCURE

CONTROLLED//SP-AIV/LCOMM//DL ONLY

S//CUI//SP-EXPT/EXPTR/FEDCON

The above markings are intended for demonstrative purposes only and do not describe the content of this page or presentation

The CUI Registry: https://www.archives.gov/cui/registry/category-list

- **Among other information, the CUI Registry identifies and describes all approved CUI groupings and categories and includes 20 general "Organizational Index Groupings" (OIGs) under which multiple categories of CUI are organized**
  - Note that CUI is controlled at the "category level" only;
  - OIGs serve as a method for grouping categories of CUI and are not used to control CUI

OIG	Categories
Critical Infrastructure	Information Systems Vulnerabilities; Water Assessments
Financial	Comptroller General; Bank Secrecy; Budget
Intelligence	Agriculture; Geodetic Product Information
Law Enforcement	Terrorist Screening; Legal Privilege

Critical Infrastructure	NATO
Defense	Nuclear
Export Control	Patent
Financial	Privacy
Immigration	Procurement and Acquisition
Intelligence	Proprietary Business Information
International Agreements	Provisional
Law Enforcement	Statistical
Legal	Tax
Natural and Cultural Resources	Transportation

- **All CUI is subject to minimum safeguards, but some are afforded specific handling and dissemination instructions required by law or policy**
- **Why is this distinction important?**
  - Differing handling and dissemination requirements
  - Differing marking requirements

The CUI Registry

CUI Category: General Procurement and Acquisition

Category Description:	Material and information relating to, or associated with, the acquisition and procurement of goods and services, including but not limited to, cost or pricing data, contract information, indirect costs and direct labor rates.
Category Marking:	PROCURE
Banner Format and Marking Notes:	Banner Format: CUI//Category Marking//Limited Dissemination Control Marking Notes: • Category Marking is optional when marking Basic CUI unless required by agency policy. Example: CUI//Limited Dissemination Control • Category Marking preceded by "SP-" is required when marking Specified CUI. Example: CUI//SP-Category Marking//Limited Dissemination Control • Whether CUI is Basic or Specified is determined by the applicable Safeguarding and/or Dissemination Authority for a given instance of CUI. • Separate multiple Category Markings by a single forward slash (/) and list Category Markings alphabetically. Example: CUI//Category Marking A/Category Marking B//Limited Dissemination Control • Category Markings for Specified CUI precede Category Markings for Basic CUI. Example: CUI//SP-Category Marking/Category Marking//Limited Dissemination Control • Separate multiple Limited Dissemination Controls by a single forward slash (/). Example: CUI//Category Marking//Limited Dissemination Control/Limited Dissemination Control • Reference 32 CFR 2002.20 , CUI Marking Handbook , Limited Dissemination Controls and individual agency policy for additional and specific marking guidelines.

e.g. **"CONTROLLED//SP-PROCURE"**

Notes for Safeguarding, Dissemination and Sanction Authorities:

- **CUI Specified authorities include specific handling practices that differ from general CUI requirements. For Specified authorities, reference individual Safeguarding/Dissemination control citations for distinct requirements**
- Whether CUI is Basic or Specified is determined by the applicable Safeguarding and/or Dissemination Authority for that CUI.
- Each "Safeguarding and/or Dissemination Authority" citation links to the statute, regulation or government-wide policy authorizing the control of that information as CUI.
- Each "Sanctions" authority links to the statute, regulation or government-wide policy that includes penalties for CUI misuse of CUI for the associated "Safeguarding and/or Dissemination Authority" on the same line.

Safeguarding and/or Dissemination Authority	Basic or Specified	Sanctions
48 CFR 3.104-4	Specified	41 USC 2105 48 CFR 3.104-8
48 CFR 52.215-1(e)	Specified	41 USC 2105 48 CFR 3.104-8

Two standards for handling and disseminating CUI: "CUI Basic" and "CUI Specified"

- CUI Basic – Law, regulation, or government-wide policy identifies an information type and says to protect it
- CUI Specified - Law, regulation, or government-wide policy identifies an information type and says to protect it…**and includes specific handling standards for that information**

Defense CUI

- **There are four categories of Defense CUI:**
  - Controlled Technical Information
    - (CUI//**SP**-CTI)
    - Safeguarding and/or Dissemination Authority: DFARS 252.204-7012
  - DoD Critical Infrastructure Security Information
    - (CUI//DCRIT)
    - Safeguarding and/or Dissemination Authority: 10 U.S.C. 130(e)
  - Naval Nuclear Propulsion Information
    - (CUI//**SP**-NNPI) or (CUI//NNPI)
    - Safeguarding and/or Dissemination Authority: 42 U.S.C. 2013 ***or*** 50 U.S.C. 2511
  - Unclassified Controlled Nuclear Information – Defense
    - (CUI//**SP**-DCNI) or (CUI//DCNI)
    - Safeguarding and/or Dissemination Authority: 10 U.S.C. 128(a) ***or*** 42 C.F.R. 223

SO, YOUR DOD CUSTOMER GAVE YOU "CUI." COOL. WHICH ONE?

Records and Documentation

It isn't about the documents

It's about protecting CUI and your operations

by getting the correct people

to perform specific tasks

on a specific schedule

consistently

and finding / fixing deficiencies

Does your documentation help you do these things?

System Security Plan

- Most important compliance document
- Normally 100-300 pages long for small / medium businesses
- May be split into multiple documents
- Identifies what you are trying to protect (CUI)
- Describes your network and major protective systems
- Provides in-depth answers addressing how you perform each security requirement (800-171 / CMMC) to protect CUI
- Used extensively during self- and 3rd-party assessment

https://www.cmmcaudit.org/system-security-plan-for-800-171-and-cmmc/

Policies

- Policies show intention to perform requirements
- Procedures provide evidence your manual tasks correctly & effectively address requirements
- Policies, procedures, specifications, build instructions, user agreements, and training get staff on the same page
- Improve procedures over time to prevent process failures

Proving consistency

- **Most companies can apply technical requirements**
- **Much more difficult to consistently perform manual tasks**

1. **Create a process, template, or form to guide staff performing each repeating task**
2. **Hire more people once you know level of effort**
3. **PRIORITIZE these tasks – management support!**
4. **Use checklists, tickets, and other methods to…**
   - Trigger performing tasks on schedule
   - Ensure tasks aren't forgotten / overlooked
   - Create proof to demonstrate work was performed

Mechanics of 3rd Party Assessment

- **Initial Quote**
  - Ready? (good system security plan, self-assessed?)
  - Level of effort? (complexity, onsite visits, enclave vs enterprise)
- **Scoping and Readiness Review**
  - Review inventories, diagrams, system security plan
  - Look for common failure points (FIPS, boundaries, illogical implementation descriptions)
- **Assessment**
  - 2 weeks to prepare evidence
  - Assessment normally 1 week
- **Wrap up**
  - Detailed report, results, and notifying DoD / Cyber-AB

So you passed your 3rd Party Assessment

- **Hooray! What's next?**
- You now have a Cybersecurity program and you demonstrated with evidence you are following the program you created around the 110 controls
- Maintain your program to retain your certification
- Maintain awareness of key verbs in the standard
  - All "reviews" need to occur within assigned periodicity
  - All "updates" need to occur as required
  - "Maintain" your systems as required (Threat-based???)
  - Continuously gather evidence/proof for the next assessment
- Maintain focus and pressure on your Cybersecurity program
  - Will drive you and your team to update your posture based on evolving threats

NDIA Recommendations

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

1. **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

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

Questions?