CMMC:
Defining Controlled Unclassified Information (CUI)

Current As Of: 5 October 2022 / 1300 EDT

TODAY'S SPEAKERS

Col (Ret) Rachel McCaffrey, USAF

Senior Vice President of Membership & Chapters, NDIA

Executive Director, Women In Defense

Vince Scott

CEO

Defense Cybersecurity Group

INFRAGARD National SME Cyberwarfare

Alex Major

Attorney, McCarter and English

https://www.mccarter.com/

Sponsored by: C3 INTEGRATED SOLUTIONS

Bottom Line Up Front

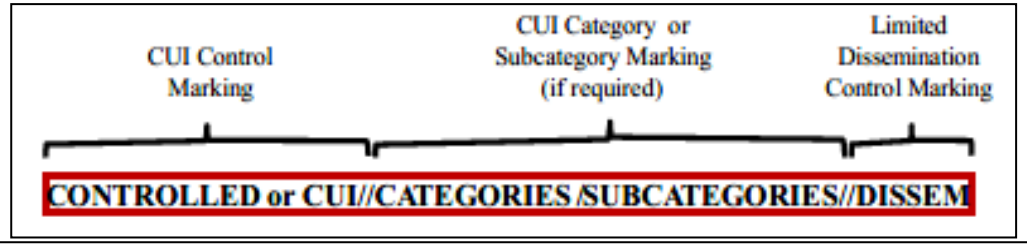
- **Secure your Networks**
- Protect **your** IP
  - Relatively easy?
- Protect the Government's identified critical unclassified information
- Misunderstanding among most stakeholders about Controlled Unclassified Information (CUI) definition
  - CUI currently very complicated; much broader than DoD-only
  - CMMC could drive default to "Everything is CUI"
- Increases scope of CMMC challenge, making it hard to develop / implement reasonable solutions

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."**

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

Sponsored by: C3 INTEGRATED SOLUTIONS

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?

Proposed CMMC CUI Criteria

- **Narrowly defined to effectively limit scope of protected information**
- **If everything is a priority, nothing is a priority**
  - We cannot effectively protect every piece of information
- **Government should base CUI determination on two factors: Category & Ownership**

Category

- **Defense CUI**
  - Controlled Technical Information
  - DoD Critical Infrastructure Security Information
  - Naval Nuclear Propulsion Information
  - Unclassified Controlled Nuclear Information – Defense
- **Other Potential Categories – within the context of DIB Acquisition and Procurement**
  - Nuclear
  - Export Control
  - ITAR

Ownership

- **Commercially developed capabilities should generally not be subject to CUI labeling**
  - Exceptions for significant technical capabilities
  - Burden of proof on the government for identify
- **Capabilities developed solely for the government or modified capabilities, modified via government contract, are subject to CUI**

Category Example

- **Your company invests/develops new electronic test capability**
  - You determine technology covered by EAR & ITAR
  - You funded the research; you own the IP so NOT CUI
- **Government likes the capability**
  - Put your company on contract to modify equipment to meet government requirements
  - Modified test capability both CUI and EAR/ITAR because qualifies as government info
  - Info includes government-furnished as part of contract requirements and info your company developed in responding to contract requirements
  - BL: If EAR/ITAR **and** Federal Info, it is (and should be marked) CUI

Category Example ***UPDATED from webinar***

- ***Court Protects Closely Guarded Vendor Lists***
  - https://www.nationaldefensemagazine.org/articles/2022/8/26/court-protects-closely-guarded-vendor-lists
- **Raytheon Company v. U.S., published by the Court of Federal Claims on June 30. (No. 19-883C; 2022 U.S. Claims LEXIS 1385; 2022 WL 2353085)**
- **Army could not direct Raytheon to declare vendor lists "technical data"**
  - Army sought very broad license to share info with any other contractor
  - Court found in favor of Raytheon; lists are not technical data
- **3 Criteria**
  - Negative competitive impact of government sharing the data
  - "Technical Data"
  - Ensure data marked to align with appropriate restrictions; no markings usually means no restrictions

Caution

- **Companies should not unilaterally mark information CUI when it is not Federal information**
  - If company proprietary, mark: “Acme Proprietary Info”
  - If you mark it CUI, you indicate you believe the info to **BE** Federal info
  - Could potentially give government claim to your proprietary info

So What? The Importance of Clear Definition

- Cannot bring focus to the problem without defining high-priority data to protect
- We cannot protect 100% of our **UNCLASSIFIED** information/data 100% of the time
- Business must understand the scope and scale of the requirement to effectively build their IT infrastructure and processes
- In the absence of clear, precise, commonly understood/recognized/agreed upon definitions, the magnitude of the problem defies reasonable solutions
- 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)

So What?

- **Can DoD organizations meet the standard with their current IT infrastructure and processes?**
  - DoD IG determined internal organizations complying with ~78% of requirements
  - Costs to achieve final 20% significantly higher in terms of time, manpower, money
  - Implementing highest priority 20% of the controls delivers significant benefit
- **Can other Executive Branch organizations?**
- **Can the Legislative Branch?**
- **Important small companies (dual use supply chain) will leave the DIB rather than pay the costs to comply**
  - "The perfect is the enemy of the good enough"
  - "When you start at 0, an 80% solution starts to look pretty good."

Final Thoughts

- **Technology** evolves; CMMC does not currently account for MSP / Cloud-based solutions
- **Threats** evolve; Security requirements evolve to mitigate threats
- **Government never eliminates any controls**
  - Some controls no longer perform the function for which they were designed
- Continuously increasing requirements drive continuously increasing costs
  - Ultimately creates opportunity costs by focusing limited DoD resources on security instead of capability and readiness
- Periodic **updates based on evolving technology** could help deliver desired outcomes at lower cost
- Periodic **pruning of controls** could help deliver desired outcomes at lower costs

Questions?