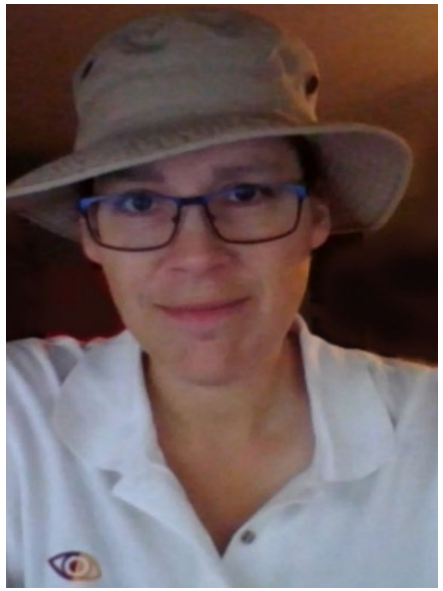
CMMC Update: Defining CUI Part I -- Overview

Current As Of: March 2024

TODAY'S SPEAKERS



Amira Armond

President

Kieri Solutions

Vice Chair, C3PAO Stakeholder Forum

Cassia Baker

Research Faculty

Georgia Institute of Technology

Ryan Bonner

CEO

DEFCERT

Alex Major

Attorney

McCarter and English

Sponsored by:

COALFIRE FEDERAL

Secure Your Networks and Systems In Physical Space and Cyberspace

- **Secure your Networks. Now**
- **Know your Contracts**
  - Your contracts should tell you what information you must protect
- **Define & Understand your business processes to identify how & where you store / handle / transmit CUI**

Why CUI?

- **Why not classified? Cost of clearances & systems**
  - EO 13526
    - **Top Secret**: "Exceptionally Grave Damage"
    - **Secret**: "Serious Damage" / **Confidential**: "Damage"
  - 2.95M US government employees Sep23
  - 1.1M workers in the DIB
- **Government**
  - Established by EO13556, CUI program standardizes the way the executive branch handles **unclassified information** that requires safeguarding or dissemination controls pursuant to and consistent with **law**, **Federal regulations**, & **Government-wide policies**
- **DoD contractors and sub-contractors**
  - **Narrow scope**: Protect information that could provide adversaries with competitive advantage or downgrade/eliminate a competitive advantage for our warfighters
  - **Broad scope**: Protect information the government must protect in the same way the government protects it

2017 FAR case -- Unfinalized

- **2017-016 Controlled Unclassified Information implements:**
  - 1) NARA CUI program of E.O. 13556, which provides implementing regulations to address agency policies for designating, safeguarding, disseminating, marking, decontrolling, and disposing of CUI;
  - 2) OMB Memorandum M-17-12, Preparing for and Responding to a Breach of PII (January 3, 2017) which provides guidance on PII breaches occurring in cyberspace or through physical acts.
- **Status: 08/04/2022 FAR and DARS Staffs resolving open issues identified during OIRA review**
  - Until yesterday…when the FAR CUI rule began moving again
  - FAR CUI rule – create clause requiring ALL federal contractors to protect CUI

Defining Controlled Unclassified Information (CUI)

- **Federal Contract Information (FCI)**
  - "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)**
  - 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 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

Defining CUI – CUI vs FCI

- "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**."
- **All CUI in possession of a Government contractor is FCI**
- **Not all FCI is CUI**
- **Technical information marked "CUI" can imply the information belongs to the government**
- **Non-government contractors producing innovative technical information do not mark anything CUI**

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

- **Among other information, the CUI Registry identifies and describes 20 general "Organizational Index Groupings" (OIGs) under which 126 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

Defining CUI: 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**

Sponsored by:

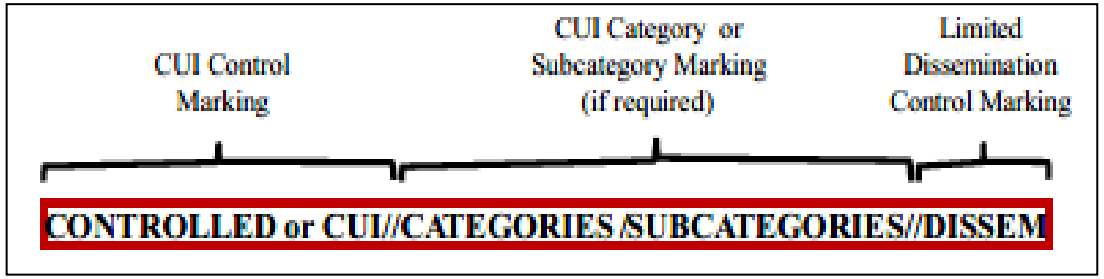
COALFIRE FEDERAL

9 Alex

Defining CUI – Come on, does it really matter?

- **Yes. Yes, it does.**
- **Sidestep: DOE HQ Facilities Master Security Plan Ch 13**
  - Updated in January 2024; Outlines DOE CUI Program IAW DOE Order (O) 471.7, *Controlled Unclassified Information*
  - "Provides basic information on CUI and Unclassified Controlled Nuclear Information (UCNI)."
  - "UCNI is certain unclassified design and security information concerning nuclear facilities, material, and weapons that are controlled under the Atomic Energy Act."
  - "Because of the sensitivity of the information, very specific requirements for UCNI are in Title 10 Code of Federal Regulations Part 1017 and DOE O 471.1B."
  - "Therefore, UCNI must continue to be reviewed, identified, marked, and protected as required under these policies ***and must not be marked under CUI policies*** (e.g., CUI//SP-UCNI)."
  - "No other CUI markings are required on documents containing UCNI."
  - "For clarification, [In this Chapter 13] each section addresses CUI and UCNI separately."

Defining CUI – Examples of Correct Marking



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

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***
  - Privileged Safety Information
    - CUI//PSI
    - Safeguarding and/or Dissemination Authority: ***10 USC 184 - Joint Safety Council*** or P.L. 115-232 (FY 2019 National Defense Authorization Act) Section 1087(j)
  - Unclassified Controlled Nuclear Information – Defense
    - (CUI//**SP**-DCNI) or (CUI//DCNI)
    - Safeguarding and/or Dissemination Authority: ***10 U.S.C. 128(a) or 32 C.F.R. 223***
      - ***10 USC 128*: Control and physical protection of special nuclear material: limitation on dissemination of unclassified information**
      - ***32 CFR 223.6*: Procedures-identifying and controlling DoD UCNI**

Other potentially relevant categories of CUI

- **Within the context of DIB Acquisition and Procurement**
  - Export Control
  - ITAR
  - Proprietary
- **Other categories**
  - HIPAA – Does your company have a contract with DHA?
  - PII
- **Know your contracts**
  - WHAT must you protect?
- **Know your processes**
  - What is the information flow (store / handle / transmit)

What should organizations DO?
CUI You Receive or Create

- **Know your Contracts**
- **Know your Processes**
- **Expectation government will properly mark information**
- **Marked and Organization agrees it is CUI**
  - Handle it appropriately, even if government did not (encryption)
- **Not marked but "looks like CUI"**
  - Best effort
- **Educate your workforce on your contract**
  - Ensure they can identify CUI and understand required processes to protect it

CMMC Assessment scope begins with business processes

- **Business processes drive CUI store / handle / transmit**
- **In addition to IT / Systems / Networks, Assessment scope also includes:**
  - People
  - Facilities
  - 3rd Parties
  - Tooling / Capital Equipment / OT / IoT
- **Business and functional managers must understand and track business process support systems, applications, and services**
- **Must know what information you are required to protect to determine scope**

Why is CUI important? An Assessor's perspective

- **Assessors unlikely to deep dive on CUI**
- **Will request high-level info about information company stores / handles / transmits**
  - Export Controlled
    - Control the flow of CUI
    - Control/verify the use of external systems
- **Default: treat all CUI the same**
- **Focus: Strong boundaries / procedures / security**
- **Assessor will document company's stated "CUI Scope" and assess based on company assertion**
- **Assessor should not mark a company deficient if**
  - Not marked properly (not the company's fault)
  - Originated outside the company

Questions