CMMC Update:
Defining CUI
Part II – Operational Implications

Current As Of: April 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

Sponsored by:

COALFIRE FEDERAL

TODAY'S SPEAKERS

Alex Major

Attorney, McCarter and English
https://www.mccarter.com/

Vince Scott

CEO
Defense Cybersecurity Group
INFRAGARD DIB Sector

Sponsored by:

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
- **Established by EO13556, Controlled Unclassified Information (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**
- **Define & Understand your business processes to identify how & where you store / handle / transmit CUI**

Defining CUI – NDIA Proposals for Government

- **Limit scope**
  - Non-Government organizations should not have to meet all Government requirements
- **Clearly define information requiring safeguarding**
  - Mark properly when disseminating
- **Clearly define from whom industry is safeguarding the information**
  - AUKUS?
- **Clearly Define Requirements**
  - Clearance – CUI is unclassified, so no clearance required?
  - Signed Non-Disclosure Agreement (no sharing) – Contract?
  - Need to Know – Who determines need to know, especially with regard to non-US persons?
    - "Can a US Entity share technical documents with Distribution statement D to a parent or subsidiary Foreign entity (as identified in SAM)?"

NDIA Industry Feedback: What do companies need to protect?

- **Protection required for a vast array of data**
  - Should:
    - Banking information
    - YOUR Intellectual Property (IP)
      - Everyone on your team should be able to ID & mark PROPIN
      - Do not unilaterally mark your IP CUI
    - Supply chain sources and methods (business email compromise)
    - IT infrastructure buildout
  - Must:
    - HR Information (PII/PHI/HIPPA etc. – required by law)
    - Classified information
    - Federal Contract Information (FCI) – Contractual Obligation
    - Controlled Unclassified Information (CUI) – Contractual Obligation

Defense CUI

- **There are five 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**

Marking Documents

- **Mismarking – Email, documents, briefing slides, websites**
  - Unmarked CUI
  - Overmarked CUI
  - Incorrectly marked CUI
- **Make it easier for your customers and staff (tips)**
  - Create marking templates for each program you support, for the specific CUI included in the program
  - Identify correct Authorities and POCs for each program (pro tip: reference correctly labeled CUI documents you've already got)
  - Templates should include full Designation Indicator blocks
  - Templates should include instructions for Email, PowerPoint, Word Documents, large prints, and software code

Identifying CUI: Ownership & Possession

- **Government should base defense CUI determination on two factors: Category & Ownership / Possession**
- **Commercially developed capabilities should generally not be subject to CUI labeling**
  - Exceptions for significant technical capabilities?
  - Burden of proof on the government to identify
- **Capabilities developed solely for the government or modified capabilities, modified via government contract, are subject to CUI**

Ownership & Possession Example

- **Your company invests in / develops new electronic test capability**
  - You determine technology covered by EAR & ITAR
  - You funded the research; you own the IP so NOT CUI

Ownership & Possession – Possible Outcome 1

- **Government likes the capability**
  - Puts your company on contract to modify equipment to meet government requirements
  - Modified test capability is a specially designed defense article (ITAR technical data)
  - Government enjoys unlimited rights for test capability information (it is not proprietary)
  - Result: this information is CUI
- **Markings**
  - Government instructs your company to mark deliverable(s) as CTI & EXPT
  - Your company adds CUI designation indicator with CTI & EXPT
  - Your company adds an export control warning statement

Ownership & Possession – Possible Outcome 2

- **Government likes the capability**
  - Puts your company on contract to modify equipment to meet government requirements
  - Modified test capability is a specially designed defense article (ITAR technical data)
  - Your company negotiates Limited Rights for test capability information (***it is proprietary***)
  - Result: the information is not CUI for you but will be marked as CUI when possessed by the Government
- **Markings**
  - Government instructs your company to mark the deliverable(s) as CTI and EXPT
  - Your company adds a CUI designation indicator with CTI, EXPT, and PROPIN (Proprietary Business Information) ***to the copy you provide as a deliverable***
  - Your company adds mandatory Limited Rights restrictive markings to the copy you provide as a deliverable / all copies of the information.*
  - Your company adds an export control warning statement to all copies of the information

Questions