CONTROLLED UNCLASSIFIED INFORMATION:.

DCSA CUI Update

Fall FISWG/NCMS Training Event

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

Lilian Benitez
CUI Branch Action Officer
Enterprise Security Operations
DCSA Industrial Security

Agenda

- Why CUI is Important to Industry
- Federal Acquisition Regulation (FAR)
- Defense Federal Acquisition Regulation Supplement (DFARS)
- Making sense of what is CUI
- Understanding the Cybersecurity Maturity Model Certification (CMMC)
- DCSA role within the CUI Mission Space
- Clarifying CUI responsibilities within the National Industrial Security Program
- What we discovered from the Contractual Requirements Review (CRR) pilot

Why CUI is Important to Industry

- National Security
  - Historically, CUI has been the path of least resistance for adversaries. Loss or compromise of aggregated CUI is a risk to the effectiveness of our warfighters
  - Industry support National Security
  - Policy driven

- Financial
  - Impacts the bottom line to stay in business
  - Protect proprietary Information

- Personal
  - Personal information has been breached
  - It could be misused

FAR Contractual Requirements

FAR 4.1903 Contract clause.

Contracting officers will include FAR 52.204-21 in solicitations and contracts when the contractor or a subcontractor at any tier may have Federal contract information residing in or transiting through its information system.

FAR 52.204-21 Basic Safeguarding of Covered Contractor Information (FCI) Systems.

This clause establishes the 15 basic requirements and procedures for safeguarding FCI within covered contractor information systems.

DFARS Contractual Requirements

Safeguarding & Reporting

- DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting

Assessments

- DFARS 252.204-7019 Notice of NIST SP 800-171 DoD Assessment
- DFARS 252.204-7020 NIST SP 800-171 DoD Assessment Requirements

Defense Federal Acquisition Regulations Supplement

Cyber Maturity Model Certification

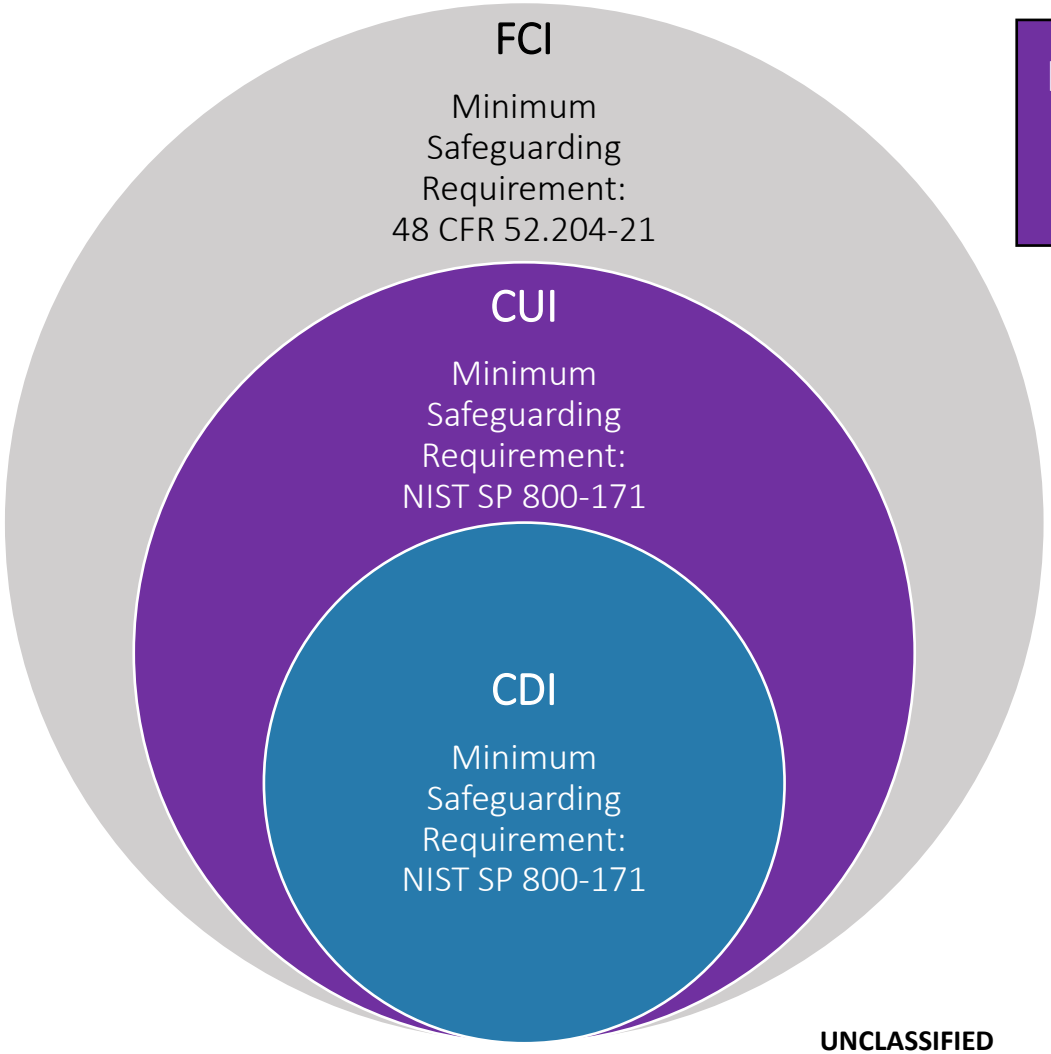
- DFARS 252.204-7021 Contractor Compliance with the Cybersecurity Maturity Model Certification (CMMC) Level Requirement.

Supplier Performance Risk System

- DFARS 252.204-7024 Notice on the Use of the Supplier Performance Risk System

FCI, CUI & CDI: Make It Make Sense

Safeguarding Requirements for Non-Federal Information Systems



Information that is not marked as public or for public release

Information that is marked or identified as requiring safeguarding in the DOD CUI Program

Information identified in accordance with DFARS 252.204-7012

Public Information
Public Information or information marked for public release.

CMMC Familiarization

- Become familiar with NIST SP 800-171, Protecting Controlled Unclassified Information in Non-federal Systems and Organizations and DoD CMMC 2.0

- CMMC stands for “Cybersecurity Maturity Model Certification” and is a unifying standard for the implementation of cybersecurity across the Defense Industrial Base (DIB).

- The CMMC framework includes a comprehensive and scalable certification element to verify the implementation of processes and practices associated with the achievement of a cybersecurity maturity level.

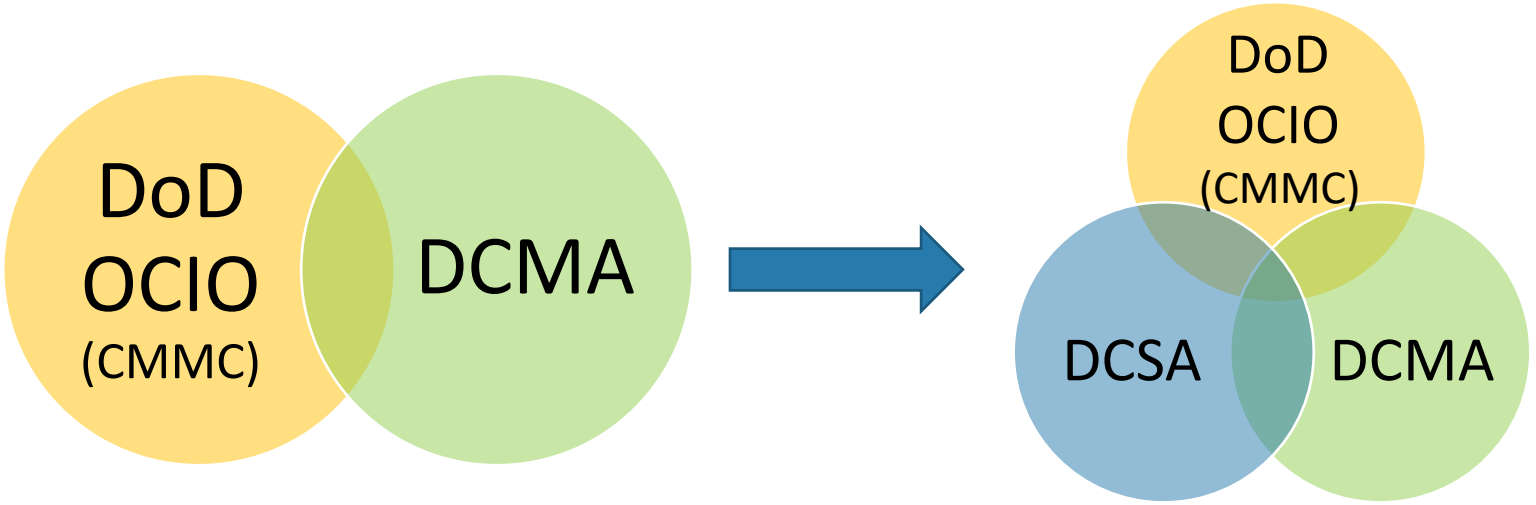
- CMMC is designed to provide increased assurance to the Department that a DIB company can adequately protect sensitive unclassified information, accounting for information flow down to subcontractors in a multi-tier supply chain.

- CMMC 2.0 is in alignment with section 4.1901 and the 15 requirements identified in FAR 52.204-21 which are aligned with self assessment requirements of CMMC level 1 and NIST SP 800-171.

- Two proposed CMMC rules have been published for public comment that will further the clarify the CMMC process as the CUI program matures with in the DoD.

The DCSA Role

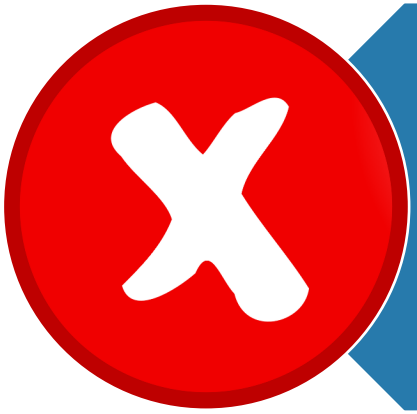
- DODI 5200.48 assigns eight (8) CUI mission responsibilities to DCSA
- CUI Assessments are not new
  - DoD OCIO: Cybersecurity Maturity Model Certification (CMMC)
  - DCMA: NIST SP 800-171 Compliance Assessments



CRR Pilot

This was:

- Not Scored
- An overlay to the Security Review
- Data Driven
- Relationship Lead
- Risk Snapshot



This was not:

- A Technical controls assessment
- “Gotcha” Moment
- Impacting the Security Review timelines or scores

Clarifying CUI Responsibilities in the NISP

- Requirement to Access CUI
- Non-contractual CUI
- Unauthorized Disclosure (UD)
- Marking
- General Safeguarding
- CUI Training Validation

Available Resources for Industry

Resources are available!
- DOD CUI Website: www.dodcui.mil
- CDSE CUI Toolkit: www.cdse.edu
- DCSA Website: www.dcsa.mil

DCSA Website Resources
- DCSA CUI 101
- DCSA CUI Roadmap to Compliance
- DCSA CUI Industry Requirements
- DCSA SPP Template
- DCSA Security Controls Playbook
- DCSA and DoD CUI Marking Job Aids
- CUI Quick Reference Guide
- And more…

Contact Us
DCSA ESO CUI Branch operates a mailbox and a hotline where Industry may ask questions about implementing CUI safeguards:
Mailbox: dcsa.quantico.ctp.mbx.eso-cui@mail.mil
Hotline: (571) 305-4878

Questions

DCSA CUI Branch Hotline: (571) 305-4878

DCSA CUI Branch Email: dcsa.quantico.ctp.mbx.eso-cui@mail.mil