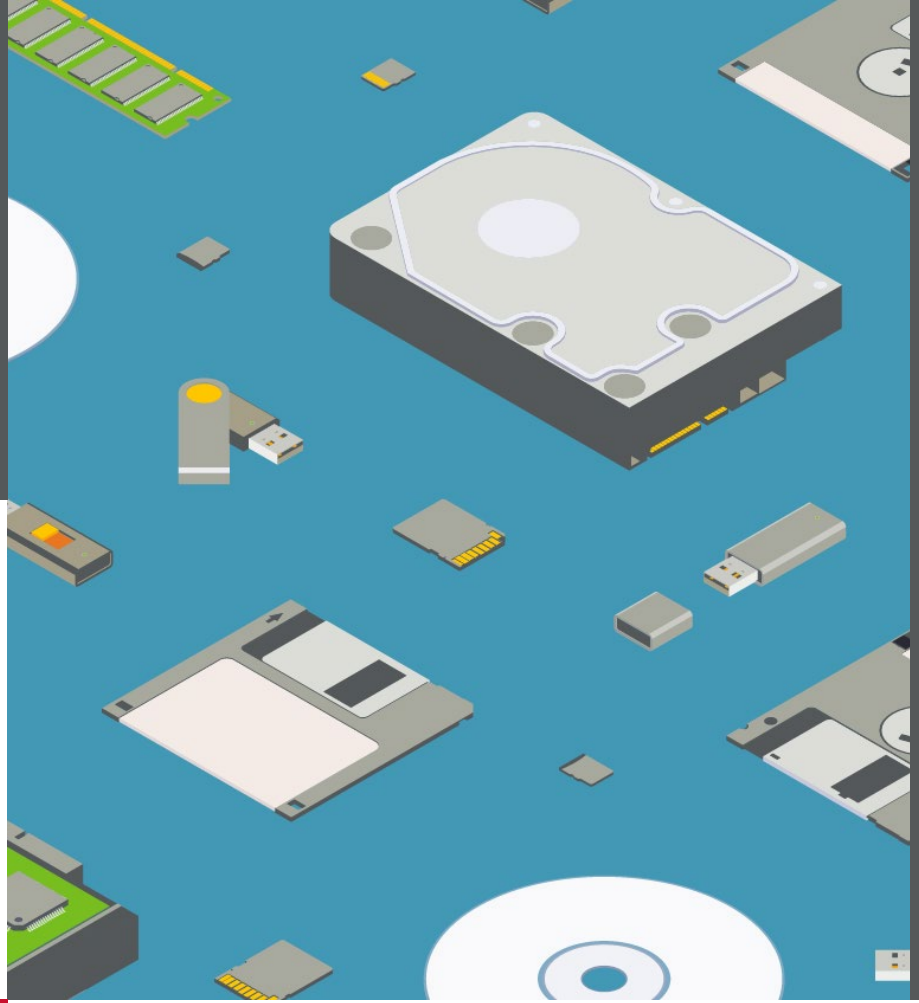
Updates to Controlled Unclassified Information (CUI) and DoD Requirements to Protect CUI



Controlled Unclassified Information Executive Summary

- Controlled Unclassified Information (CUI) is all unclassified information throughout the executive branch that requires any kind of safeguarding or dissemination control.
  - CUI is a subset of Covered Defense Information (CDI); other subset is CTI
- Federal agencies have historically had their own programs, markings, and rules which hinders sharing of information and introduces risks.
  - DoD's program was already called "CUI"; now called the Legacy CUI (e.g., FOUO)
- Executive Order 13556 mandated new Federal Government CUI Program
- Title 32 Part 2002 of the Code of Federal Regulations is the Primary Governing Document for the CUI Program for All Federal Agencies
- NIST SP 800-171 was created to protect CUI stored on non-federal IT systems
  - NIST SP 800-53 applies to CUI on Federal IT Systems; FEDRAMP reqts apply to cloud

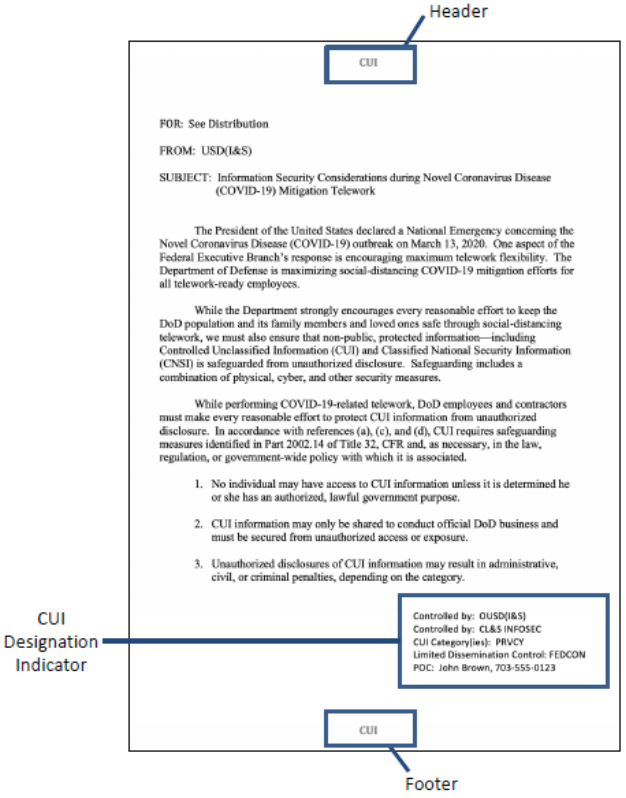
CUI Executive Summary (cont'd)

- The National Archives and Records Administration (NARA) Information Security Oversight Office (ISOO)is the Executive Agent to implement the Order and oversee agency actions to ensure compliance.
  - Established the CUI Registry Website and CUI Blog Site to Facilitate Implementation and Provide Resources
  - Provides annual updates to President
- Multiple FAR and DFAR Clauses Have Been Issued to Protect Information
  - 48 CFR 52.204-21: Basic Safeguarding of Covered Contractor Information Systems
    - Outlines minimum safeguarding measures required for Federal Contract Information (FCI)
    - Requires flow-down to subcontractors if they will also handle FCI
    - CMMC Level 1 maps to these requirements
  - 48 CFR 252.204-7012: Safeguarding Covered Defense Information and Cyber Incident Reporting
    - Standard clause in DoD contracts that must be flowed down to subcontractors
    - Mandates compliance with NIST SP 800-171; reporting cyber incidents via DIBNet within 72 hrs
    - Required compliance and self-certification by December 31, 2017

CUI Markings

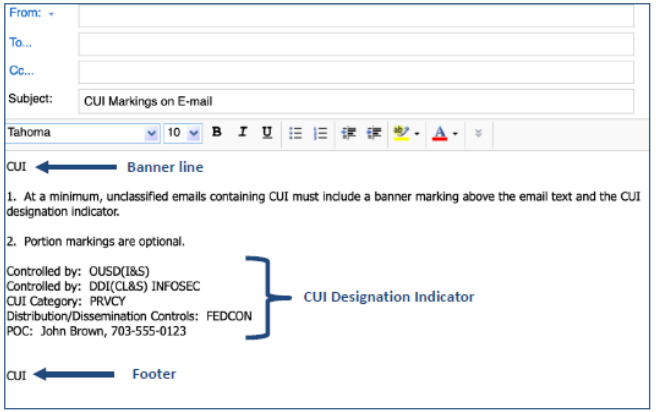
CUI Markings for Unclassified Documents

Example of markings on a CUI document without portion markings.

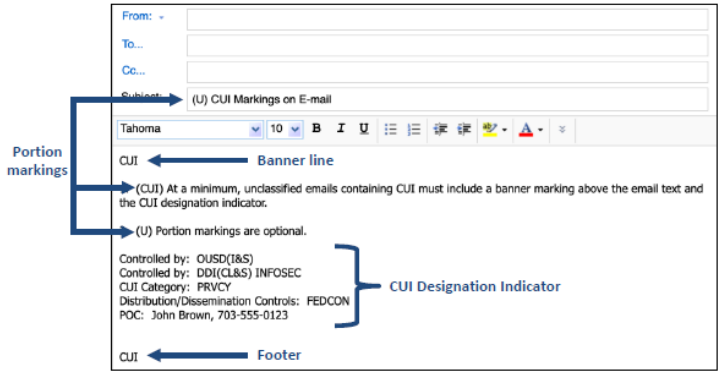


CUI Markings for Unclassified Documents

Mandatory markings

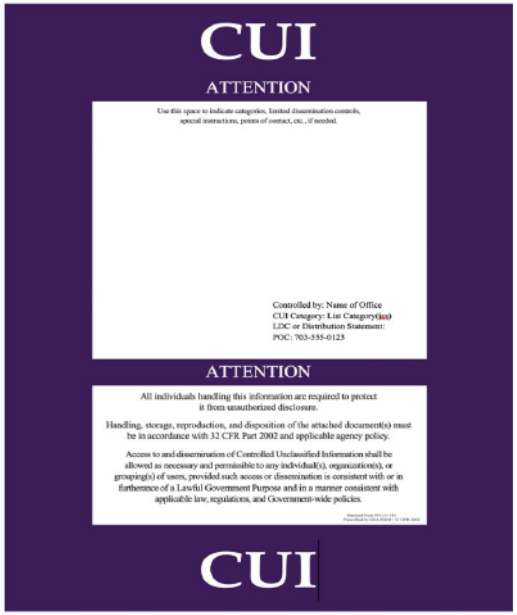


Portion markings included



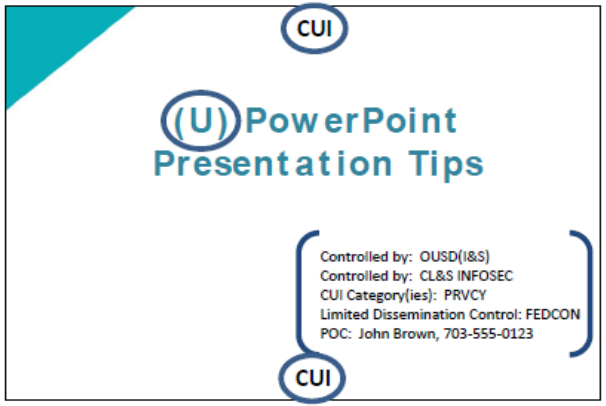
CUI Markings (cont'd)

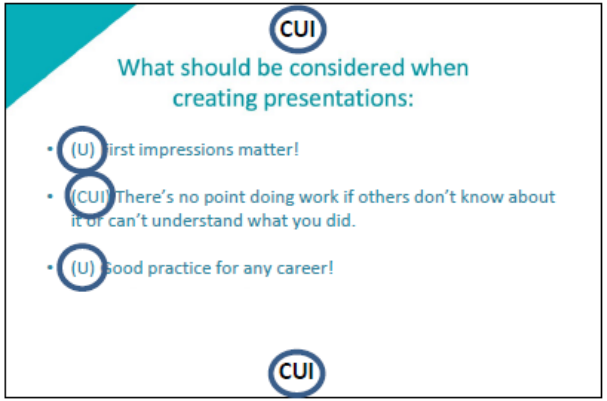
Cover Sheet and Label



SF 901, CUI Cover Sheet

SF 902, CUI Label





DoD Increased Requirements to Protect CUI

- Released Updated DoD Instruction 5200.48 on CUI
  - Mandates Annual Training (available on DoD website) & establishes DoD CUI Registry
  - Not retroactive to DoD legacy CUI program; old CUI isn't automatically new CUI
  - Assigns DCSA to administer DoD CUI Program for classified contracts
  - Section 5 is written for Industry

- New DFARS Clauses Outlining Assessment Requirements and CMMC
  - See below and next page for descriptions

- Cybersecurity Maturity Model Certification (CMMC)
  - DoD program created due to lack of consistency and rigor in contractors complying with DFARS and other requirements to protect CUI
  - Recently Change from 1.0 to 2.0 to ease burden and expenses to Federal contractors
  - Contractors desiring award of a DoD contract will have to be externally certified between Level 1-5 prior to award
    - Level 1: minimum required to receive/store Federal Contract Information (FCI)
    - Level 2: minimum required to receive/store CUI

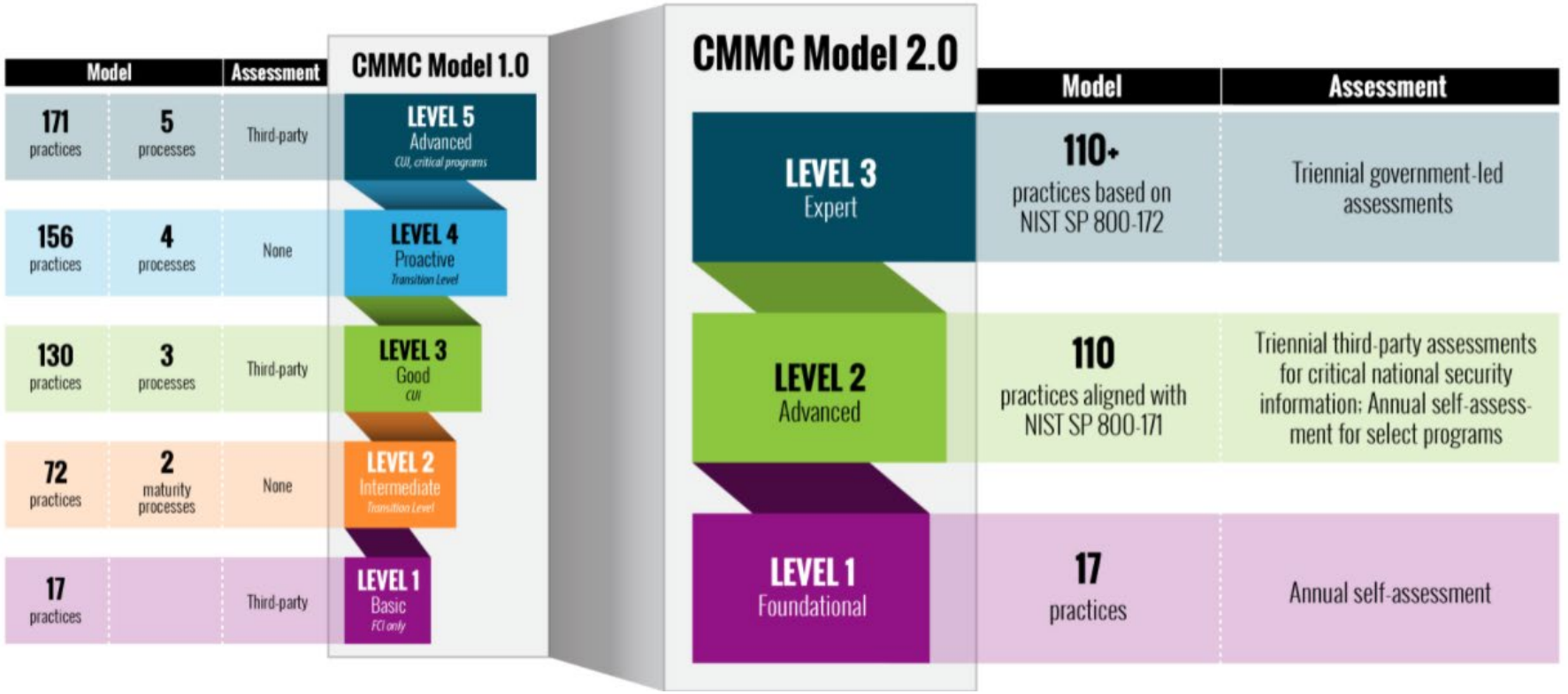
Recent Changes to DFARS

- 48 CFR 252.204-7019: requires contractors to have a DoD Assessment completed at least every three years and prior to contract award.
  - At a minimum, contractors who will work with CUI must do a self-assessment and document results in Supplier Performance Risk System (SPRS)
  - A Basic Assessment is a self-assessment completed by the contractor, while Medium or High Assessments are completed by the Government.

- 48 CFR 252.204-7020: requires contractors to allow the government access to their facility, systems, and personnel in order to conduct a Medium or High Assessment. Requires Primes to ensure their subcontractors have a proper and current assessment on file.

- 48 CFR 252.204-7021: requires contractors have a CMMC level equivalent to the sensitivity of the information expected on the contract and maintain that level of compliance for the duration of the contract.

Summary of Changes to CMMC



CMMC 2.0 Model

CMMC 2.0 model is streamlined to three versus five levels

- **Eliminates CMMC 1.0 Levels 2 and 4:** Developed as transition levels and never intended to be assessed requirements
- **Establishes three progressively sophisticated levels, depending on the type of information:**
  - Level 1 (Foundational) – for companies with FCI only; information requires protection but is not critical to national security
  - Level 2 (Advanced) – for companies with CUI
  - Level 3 (Expert) – for the highest priority programs with CUI

Requirements will mirror NIST SP 800-171 and NIST SP 800-172

- **Eliminates all CMMC unique practices and maturity processes:** Work with NIST to address identified gaps in the NIST SP 800-171
- **Aligns Level 2 with NIST SP 800-171**
- **Level 3 will use a subset of NIST SP 800-172 requirements**

Simplifies the CMMC standard for companies, while safeguarding critical Department information

CMMC 2.0 Assessments

CMMC Level 1 (Foundational) will require DIB company self-assessments

CMMC Level 2 (Advanced) may require third-party or self-assessments, depending on the type of information

- **Requires third-party assessments for prioritized acquisitions:** Companies will be responsible for obtaining an assessment and certification prior to contract award
- **Requires self-assessments for other non-prioritized acquisitions:** Companies will complete and report a CMMC Level 2 self-assessment and submit senior official affirmations to SPRS

CMMC Level 3 (Expert) will be assessed by government officials

Eases assessment requirements for companies not handling information related to prioritized acquisitions

Allowance of POA&Ms and Waivers

CMMC 2.0 will allow limited use of POA&Ms

- **Strictly time-bound:** Potentially 180 days; Contracting Officers can use normal contractual remedies to address a DIB contractor's failure to meet their cybersecurity requirements after the defined timeline
- **Limited use:** Will not allow POA&Ms for highest-weighted requirements; will establish a "minimum score" requirement to support certification with POA&Ms

Waivers will be allowed on a very limited basis, accompanied by strategies to mitigate CUI risk

- **Only allowed in select mission critical instances:** Government program office will submit the waiver request package including justification and risk mitigation strategies
- **Strictly time bound:** Timing to be determined on a case-by-case basis; Contracting Officers can use normal contractual remedies to address a DIB contractor's failure to meet their cybersecurity requirements after the defined timeline
- **Will require senior DoD approval** to minimize potential misuse of the waiver process

Limited use of POA&Ms and waivers could allow the Department and DIB companies flexibility to meet evolving threats and make risk-based decisions

Rulemaking – Codifying CMMC 2.0

Changes will be released through a interim rule. A 60-day public comment period and concurrent congressional review will be included prior to the rule becoming effective

- DoD has **mandatory rulemaking obligations** for CMMC that must be addressed as part of the CMMC 2.0 implementation
  - Rulemaking under 32 CFR is required to establish the CMMC program
  - Rulemaking under 48 CFR is required to update the contractual requirements in the DFARS to implement the CMMC 2.0 program
  - The DoD is suspending the CMMC Piloting effort and mandatory CMMC certification
- Timeline to complete all rulemaking requirements will be 9 to 24 months; includes a mandatory 60-day public comment period and concurrent congressional review
  - The DoD will continue to encourage the DIB sector to enhance their cybersecurity posture during the interim period
  - The Department is exploring opportunities to provide incentives for contractors who voluntarily obtain a CMMC 2.0 Level 2 certification in the interim period
  - Until rulemaking formally implements CMMC 2.0, the DIB's participation in CMMC will be voluntary

Methods DoD Will Utilize to Verify Compliance

- Contracting Officers will verify in Supplier Performance Risk System (SPRS) at time of contract award
- Defense Contract Audit Agency Audits
- Defense Counterintelligence and Security Agency Audits

What About CUI for Non-DoD Federal Agencies?

- The same basic rules apply for marking CUI and protecting it on non-federal IT networks as outlined in CFR Title 32 Part 2002
- CMMC is a DoD program so self-assessments and 3rd party assessments are not required; however, these are solid methodologies and practices and a good way to demonstrate compliance to non-DoD agencies
  - Other Federal agencies likely to adopt the CMMC model and process
- The NARA CUI Registry is Best Source of Information for Non-DoD CUI Requirements and Updates on Other Federal Agencies

Summary and Recommendations

- Don’t ignore this; get smart on the CMMC and CUI Requirements
  - New DoD CUI website is great one stop shopping with hyperlinks to resources
- If you want to do work as a prime or subcontractor on a DoD contract, you will at a minimum need to become CMMC Level 1 certified
- If you want to be able to work with DoD CUI, you will need to become CMMC Level 2 certified
  - CMMC 2.0 Likely Sped Up Timeline to 2023/2024 from 2025
- Do an Assessment Soonest and Record Your Score in SPRS
  - No minimum score required and no minimum timeline to get perfect score of 110
- The amount of CUI out there is very small but will grow; Critical Infrastructure will likely be the area involving AE firms
  - Can grow beyond DoD clients as CUI can be generated by non-federal entities (most likely in the critical infrastructure category)

Links to Key References and Resources

- National Archives CUI Registry
  - https://www.archives.gov/cui
- CFR 32 Part 2002 – Controlled Unclassified Information
  - https://www.dodcui.mil/Portals/109/Documents/Policy%20Docs/CFR-2018-title32-vol6-part2002.pdf
- DoD CUI Program Website (contains links to CMMC, CDSE, NARA ISOO)
  - https://www.dodcui.mil/
- DoD CMMC Website
  - https://www.acq.osd.mil/cmmc/index.html
- DoD Procurement Toolbox with FAQs on Cybersecurity
  - https://dodprocurementtoolbox.com/faqs/cybersecurity/cybersecurity-faqs-0
- Defense Industrial Base Network (DIBNet) Portal
  - https://dibnet.dod.mil/portal/intranet/
- eresilience Website on CMMC
  - https://eresilience.com/dfars-7012/