CONTROLLED UNCLASSIFIED INFORMATION:

BUILDING YOUR STARTER CUI PROGRAM

2021 AIA/NDIA FALL CONFERENCE

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

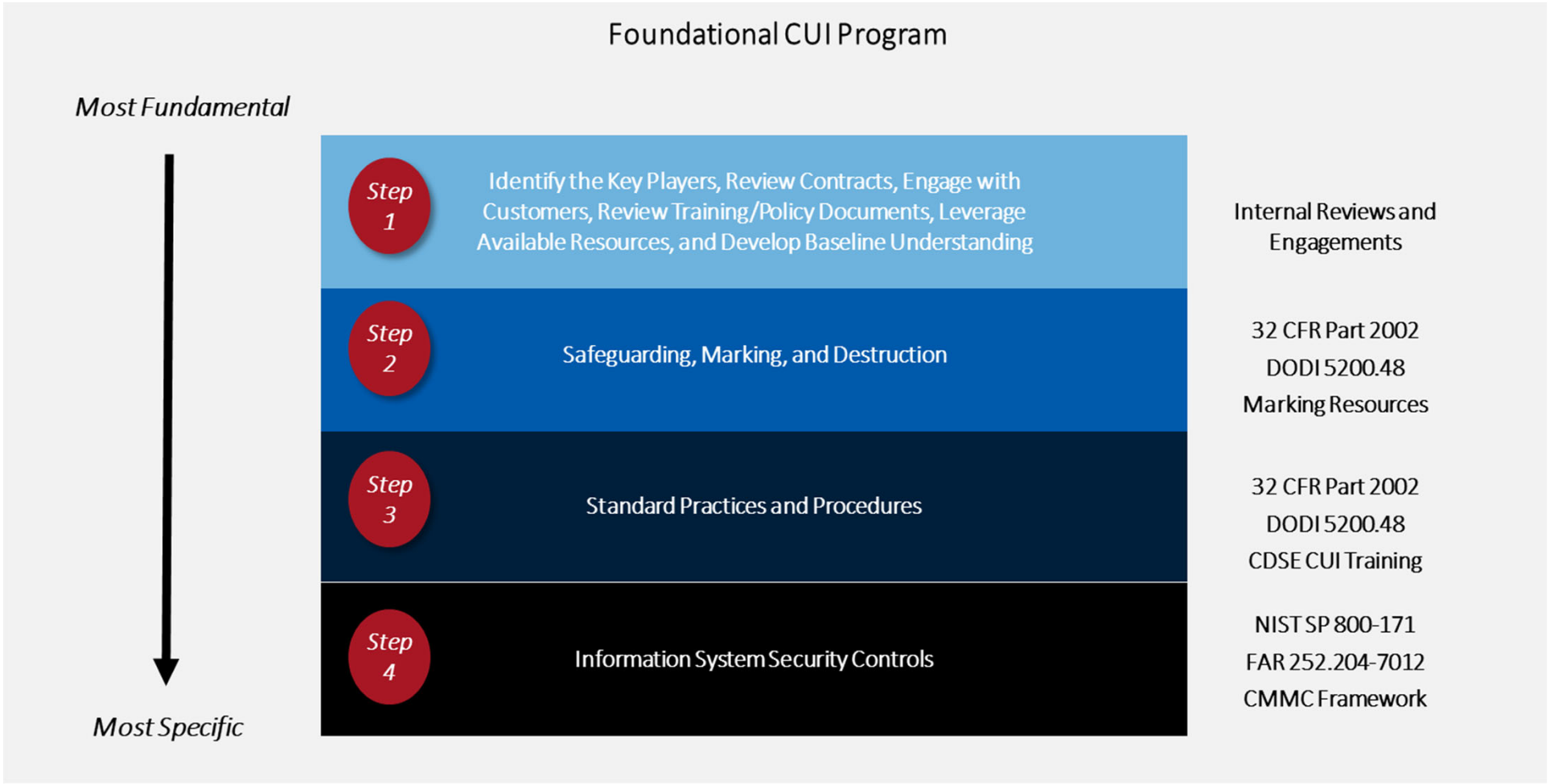
John B. Massey
Deputy Assistant Director
Enterprise Security Operations
DCSA Critical Technology Protection

APPROVED FOR PUBLIC RELEASE

Agenda

- Building the Foundation
- The Key Players
- Training and Policy Documents
- Contract Review and Customer Engagement
- Leverage Available Resources
- Standard Practices and Procedures
- Safeguarding and Destruction
- Information System Security Controls and CMMC Familiarization

Building the Foundation



The Key Players

Who are the key players in your organization's security program?

- Facility Security Officer
- Senior Management
- Insider Threat Program Senior Official
- Information Systems Security Manager
- Program Managers
- Engineers
- Contracting and Acquisition Professionals

Does your facility need a dedicated CUI Manager?

How do you educate them in CUI?

- One-Pagers
- Share DCSA resources
- Incorporate into training
- Host a brown bag luncheon
- Introduce them to the CUI Registry
- Share CDSE training course

Training and Policy Documents

Training

- DOD Mandatory CUI Training – when requested by the Government Contracting Activity when contracts contain CUI requirements
- Required annually (DOD)

Policy Documents

- EO 13556
- 32 CFR Part 2002
- NIST SP 800-171
- FAR 252.204-7012
- DoDI 5200.48

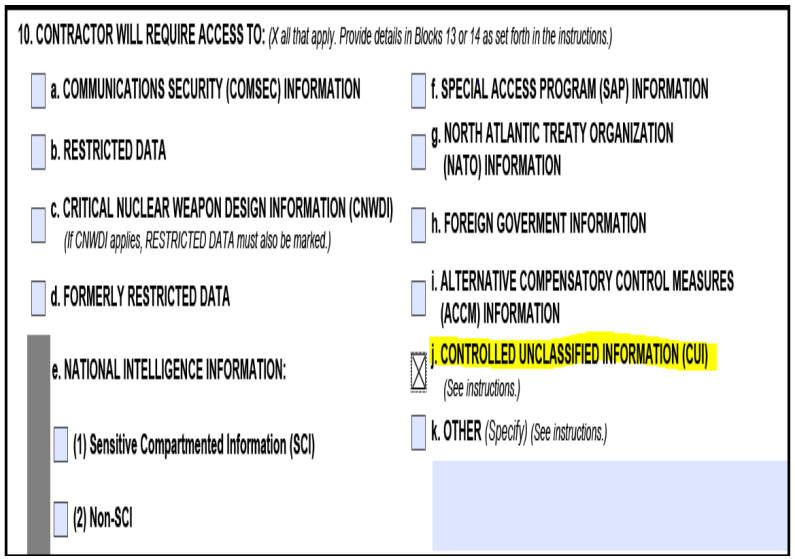
Registry Information

- National CUI Registry
- DOD CUI Registry
  - Registries support familiarization with types of information that may be CUI.
  - Registries are used by Government Contracting Activities to determine what is CUI.

Contract Review and Customer Engagement

Contract Review

- DD Form 254
  - Look for the CUI indicator in BLOCK (10 j.).
  - Look within BLOCK (13) for additional information on security requirements.
- Search other contract documents that may indicate access to CUI is required.
- If found in other documents and not listed in the DD Form 254, contact the GCA to facilitate discussion on reissuing an updated DD Form 254.
- If you believe a contract includes access to CUI but CUI requirements are not found in contractual documents (RFQ, RFP, DD 254, etc.), consult your GCA.



10. CONTRACTOR WILL REQUIRE ACCESS TO: *(X all that apply. Provide details in Blocks 13 or 14 as set forth in the instructions.)*

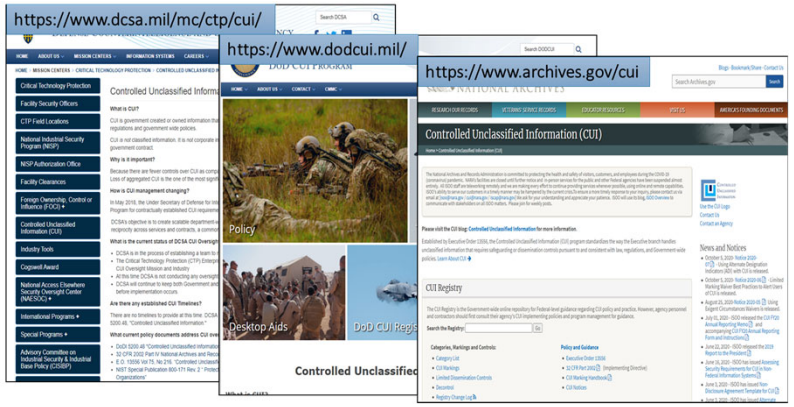
☐ a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION	☐ f. SPECIAL ACCESS PROGRAM (SAP) INFORMATION
☐ b. RESTRICTED DATA	☐ g. NORTH ATLANTIC TREATY ORGANIZATION (NATO) INFORMATION
☐ c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION (CNWDI) *(If CNWDI applies, RESTRICTED DATA must also be marked.)*	☐ h. FOREIGN GOVERMENT INFORMATION
☐ d. FORMERLY RESTRICTED DATA	☐ i. ALTERNATIVE COMPENSATORY CONTROL MEASURES (ACCM) INFORMATION
☐ e. NATIONAL INTELLIGENCE INFORMATION:	☒ j. CONTROLLED UNCLASSIFIED INFORMATION (CUI) *(See instructions.)*
☐ (1) Sensitive Compartmented Information (SCI)	☐ k. OTHER *(Specify) (See instructions.)*
☐ (2) Non-SCI	

Note: *You will likely find that each individual GCA is at a different place with implementing their CUI program and incorporating CUI requirements into contracts.*

Leverage Available Resources

Resources are available!

- DoD CUI Website: www.dodcui.mil
- NARA Website: www.archives.gov
- CDSE CUI Toolkit: www.cdse.edu
- DCSA Website: www.dcsa.mil/mc/ctp/cui/



DCSA Website Resources

- CUI Slick Sheet
- CUI FAQ
- CUI Quick Start Guide
- DCSA and DoD CUI Marking Job Aids
- NARA CUI Marking Handbook
- CUI Quick Reference Guide
- CUI Cover Sheet

- Disseminate resources to key players and have them readily available

Standard Practices and Procedures

Consider an SPP. But what would one look like?

If you have no or minimal CUI requirements…

- Baseline information and overview of CUI Program

If you have a moderate number of contracts with CUI requirements…

- Baseline information and overview of CUI Program
- Facility specific procedures
- Educational and training resources

If you a significant number of contracts with CUI requirements…

- Baseline information and overview of CUI Program
- Facility specific procedures
- Educational and training resources
- Contract-specific guidance

Safeguarding and Destruction

Safeguarding

- Follow requirements outlined in contract documentation (Block 13 - DD 254).
- To ensure CUI protection, the following measures will be implemented:
  - During working hours, steps will be taken to ***minimize the risk of access by unauthorized personnel***, such as not reading, discussing, or leaving CUI information unattended where unauthorized personnel are present.
  - After working hours, CUI information will be ***stored in unlocked containers, desks, or cabinets*** if the government or government-contract building provides security for continuous monitoring of access. If building security is not provided, the information will be ***stored in locked desks, file cabinets, bookcases, locked rooms, or similarly secured areas***.

Destruction

- CUI in all formats (hard copy, electronic, in media, etc.) will be destroyed when it is deemed to no longer to meet the threshold to be considered CUI and there are no safeguarding measures required.
- Record and non-record CUI documents may be destroyed by means approved for destroying classified information or by any other means making it unreadable, indecipherable, and irrecoverable.

Marking CUI

Leverage job aids and make them readily available to personnel actively working with CUI

Safeguarding and Destruction

Create: CUI is created when put on paper or entered into an information system.

Identify & Designate: Realize that the information is generated for or on behalf of an agency within the Executive Branch under a contract and determine if the information falls into one of the more than one hundred categories of CUI in the National CUI Registry. It is also important to realize what is not CUI.

Mark/Label: At minimum, CUI markings for unclassified DOD documents will include the acronym "CUI" or "CONTROLLED" in the banner of the document. It is a best practice to include markings in both the banner and footer of the document, and it is imperative to reference the CUI Marking Guide to ensure correct markings.

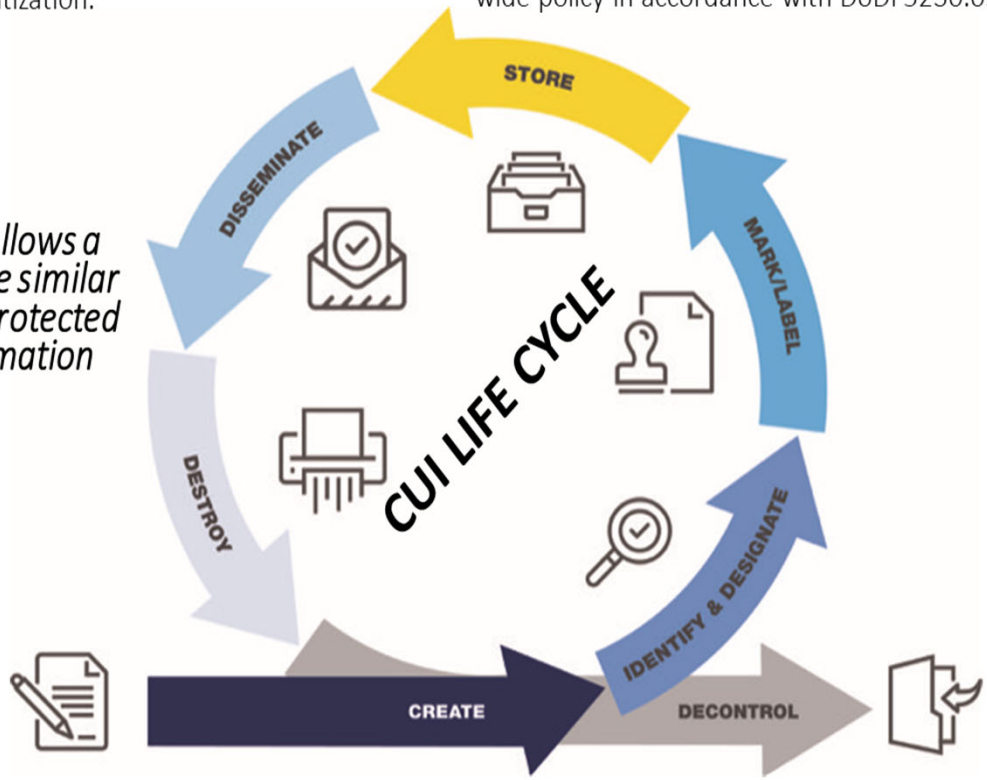
Store: CUI can be stored in NIST SP 800-171 compliant information systems or controlled physical environments.

Disseminate: Only authorized holders may disseminate in accordance with distribution statements, dissemination controls, and applicable laws.

Destroy: Hard and soft copies of CUI should be appropriately destroyed, meaning they are rendered unreadable, indecipherable, and irrecoverable. Review clearing, purging, and destruction in NIST SP 800-88: Guidelines for Media Sanitization.

Decontrol: Agencies must promptly decontrol CUI once the CUI owner has properly determined the information no longer requires safeguarding or dissemination controls, unless doing so conflicts with the related law, regulation, or government-wide policy in accordance with DoDI 5230.09.

CUI follows a lifecycle similar to all protected information



Information Security Controls / CMMC Familiarization

Information System Security Controls

- Become familiar with NIST SP 800-171, Rev 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.
- A security controls job aid is currently under development and will support implementation of 110 NIST SP 800-171 security controls.

Cyber Maturity Model Certification (CMMC)

- Become familiar with CMMC.
- 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.
- Review the CMMC FAQs: www.acq.osd.mil/cmmc/faq.html

Questions?

DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY