

Controlled Unclassified Information (CUI)

February 2023

Required Training for Access to IHMC CUI Environment

What is CUI?

- Controlled Unclassified Information (CUI) is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended.
 - CUI is a broad term established by the National Archives and Records Administration (NARA) to bundle all forms of **UNCLASSIFIED** but **Sensitive** information
 - The Executive Branch of the US Government uses over 100 terms to describe information which is both **UNCLASSIFIED** and **Sensitive**
 - ***Examples include: ITAR, EAR, PII, HIPAA, PHI, Source Selection Sensitive, Distribution D, FOUO, SBU, Sensitive Security Information, Unclassified Controlled Nuclear Information***

- Controlled Technical Information (CTI) - Technical information includes research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.
- General Intelligence (INTEL) - Related to intelligence activities, sources, or methods.
- Health Information (HLTH) - As per 42 USC 1320d(4), "health information" means any information, whether oral or recorded in any form or medium, that (A) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

For Official Use Only (FOUO) is the current DoD marking for Controlled Unclassified Information including the information processed under the Peerless Program

Implications for the Basic Research Environment

- **Cultural Change**
 - Users must consent to monitoring
 - Restrictions placed on software and network activities
 - Bring Your Own Device (BYOD) must be managed or completely prohibited
 - Privileged Users restricted to U.S. Citizens or U.S. Persons only
 - Costs associated with required monitoring hardware/software increase with larger populations of general users
 - Establishment of unique IT systems, processes and procedures for small minority or contracted activities
- **Exemptions**
 - DFAR clause 252.204-7012 allows prime contractors to exempt subcontractors who do not process “Covered Defense Information”

Implementing Protections

- The Regulations
- DoDM 5200.01 Volume 4
 - Requires annual training
 - Specifies marking requirements
 - Identifies reporting requirements
- DFAR 252.204-7012
 - Requires the use of NIST 800-171 as the standard for protecting CUI in IT systems
 - *Compliance was required on all DoD contracts 31 Dec 2017*
 - Variances must be submitted in writing to the contracting officer for consideration by the DoD CIO
 - Requires enhanced reporting of cyber security incidents
 - Requires the Federal Government to protect company proprietary information
- The Process
 - NIST publication 800-171 documents the National Institute of Science and Technology process for protecting CUI in Non-Federal institutions and organizations
 - Evaluates an organization's IT resources against 14 Security Requirement Families and proscribes detailed requirements for each

Why Protect CUI?

- Several government investigations identified a lack of security controls on unclassified systems as the number one contributor of security breaches.
 - OPM Security Breach – target of a data breach targeting personnel records, with the final estimate of stolen records totaling 21.5 million.
 - Security experts have stated that the biggest problem with the breach was not the failure to prevent remote break-ins, but the absence of mechanisms to detect outside intrusion and the lack of proper encryption of sensitive data.
 - F-35 / J-31 – Suspected industrial espionage aided the Chinese in the development of indigenous development of a stealth fighter.



- Boeing PII Exposure - An employee inadvertently leaked the personal information of 36,000 of his co-workers late last year when he emailed a company spreadsheet to his non-Boeing spouse.
 - Boeing believes the exposure to be contained to the employee and his spouse, but is providing additional training to all employees regarding the handling of sensitive information and identity theft protection services to those who's data was exposed.

CUI exposures allow the adversary access to sensitive information that may minimize any lead time advantage of US systems, or provide information regarding US personnel making them susceptible to social engineering attacks. **Known or suspected loss, compromise or unauthorized disclosure of CUI data must be reported to IHMC within 24 hours of discovery**

- IT Security

- Process and store your IHMC CUI data on the IHMC CUI Environment. Processing and storage of IHMC CUI is not authorized on personally owned or corporate systems
- Two Factor Authentication – Access to CUI processing IT systems requires something you know and something you have
- Encryption – Institute encryption on laptops and storage devices (removable and fixed) storing CUI
- PreVeil - Privileged users and all general users sending CUI over email must digitally sign and encrypt emails. The PreVeil solution provides the necessary encryption
- Network Configuration – Restrict unauthorized software; implement principle of least privilege user to remove administrator access from all regular users
- IT Auditing – Audit configurations must be adjusted to capture relevant data
- IT Monitoring – Monitoring of network and user activity required

- Training
 - Personnel must be aware of process and restrictions
 - Annual training required for all persons utilizing CUI
- Process
 - Integrate protections into holistic business processes, where required
- Physical Security
 - Validate Need – To – Know before granting access to CUI
 - Hard copies of CUI information must be locked in filing cabinets or desks when not in use. When in use, CUI must be restricted from view by unauthorized persons
- Shipping / Mailing
 - CUI may be mailed through USPS, FedEx or other mail carriers
 - Address to the proper, specific individual
 - Do Not mark the outside of the package with CUI/FOUO markings
 - Utilize package tracking

- Marking
 - Proper Markings required in all forms of information (i.e. email, hard copy, media, etc.)
 - See next slide for marking examples
- Destruction
 - Paper – Crosscut shred
 - Media – Shred/Pulverize
- Report data loss or suspected compromise to the IHMC security office immediately

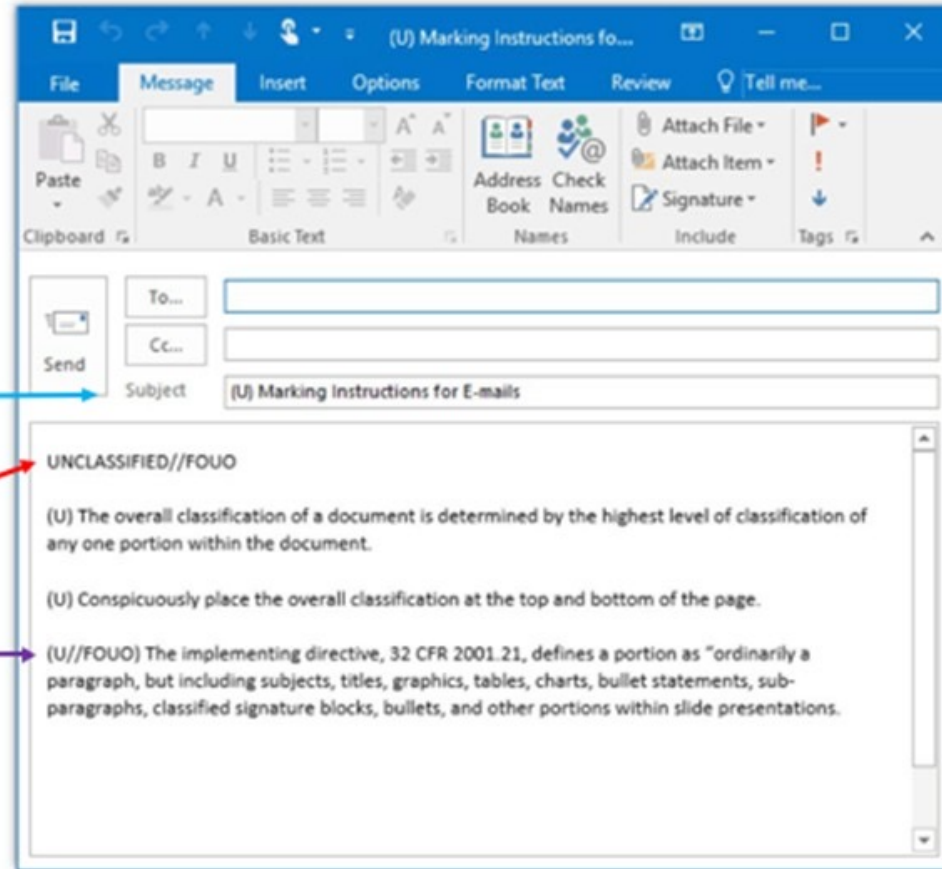
- FOUO e-mails sent external from the Agency (i.e., other than to a darpa.mil address) must be encrypted.
- All e-mails containing PII sent external from the Agency must be encrypted.

Subject/Title should indicate handling caveat (as applicable)

Must include a Banner Marking above the email text

Must portion mark FOUO or U//FOUO at the beginning of each portion containing FOUO information

Transmittal documents that have FOUO attachments shall be marked with the following statement or a similar one: "FOR OFFICIAL USE ONLY ATTACHMENT".



Marking Applied for Training Purposes Only


Marking Documents

Banner lines will be marked "UNCLASSIFIED//FOR OFFICIAL USE ONLY" in black or dark gray at the top and bottom of each page in the document.

Any subject, title, and section, part, paragraph, or similar portion that contains CUI information will be conspicuously marked with a "(FOUO)" notation.
Place the notation immediately before the text.
This will alert the reader that the information requires protection.

Distribution statement should be centered at the bottom center of every page.

UNCLASSIFIED//FOR OFFICIAL USE ONLY


 DEFENSE ADVANCED RESEARCH PROJECTS AGENCY
 875 NORTH RANDOLPH STREET
 ARLINGTON, VA 22203-0114

MEMORANDUM FOR PROGRAM SECURITY OFFICERS (PSOs)
 Subject: Controlled Unclassified Marking Examples
 Reference: DoDM 5200-01, Volume 4, "DoD Information Security Program: Controlled Unclassified Information (CUI)," February 24, 2012

(FOUO) The overall classification of a document is determined by the highest level of classification of any one portion within the document.

Conspicuously place the overall classification at the top and bottom of the page.

The implementing directive, 32 CFR 2001.21, defines a portion as "ordinarily a paragraph, but including subjects, titles, graphics, tables, charts, bullet statements, sub-paragraphs, classified signature blocks, bullets, and other portions within slide presentations.

The parenthetical notation (FOUO) will be used for sections, parts, paragraphs, or similar portions that contain For Official Use Only information. Place the notation immediately before the text.

- (FOUO) Sub-bullets should also be portion marked, especially if they are not at the same heading requirements of the parent paragraph.
 - Marking information FOUO does not automatically qualify it for exemption from public release pursuant to the FOIA.

(FOUO) All portions must be appropriate marked to indicate which portions are classified and which portions are not classified.

Word documents shall be marked "UNCLASSIFIED//FOR OFFICIAL USE ONLY" in black or dark gray at the top and bottom of every page of the document. Subjects, titles, and each section, part, paragraph, or similar portions that contain CUI information shall be conspicuously marked with the parenthetical notation "(FOUO)".

- Place this notation immediately before the text. This alerts the reader that the information requires protection.

Unclassified portions of a FOUO presentation do not require the parenthetical notation "(FOUO)".

(FOUO) Power Point briefings shall be marked "UNCLASSIFIED//FOR OFFICIAL USE ONLY" in black or dark gray at the top and bottom of the first and last slide. Internal slides of the briefing shall be marked in black or dark gray at the top and bottom to reflect the highest level of information required for that individual slide (e.g., UNCLASSIFIED or UNCLASSIFIED//FOR OFFICIAL USE ONLY).

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Distribution Statement D: Distribution authorized to Department of Defense and U.S. DoD contractors only (reason) (date of determination). Other requests for this document shall be referred to (controlling DARPA office).

Marking Applied for Training Purposes Only

Marking presentations

Banner lines will be marked "UNCLASSIFIED//FOR OFFICIAL USE ONLY" in black or dark gray at the top and bottom of each internal slide.

Any subject, title, and section, part, paragraph, or similar portion that contains CUI information will be conspicuously marked with a "(FOUO)" notation.

Place the notation immediately before the text. This will alert the reader that the information requires protection.

Portion mark all tables containing FOUO information with a "(FOUO)" notation.

Distribution statement should be placed at the bottom center of every slide.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

DARPA Sample PowerPoint Slide for FOUO Marking

- Internal slides of the briefing shall be marked in black or dark gray at the top and bottom with UNCLASSIFIED or UNCLASSIFIED//FOR OFFICIAL USE ONLY.

If there is any content on the slide that is FOUO, the marking at the top and bottom of the slide will be UNCLASSIFIED//FOR OFFICIAL USE ONLY.

(FOUO) Each portion and part of a slide shall be portion marked with a FOUO notation.

- To include all sub-bullets.
- (FOUO) And any pictures, graphs, tablets, etc.

(FOUO)

Name	Position
John Smith	PSO
Jane Doe	SETA

- Unclassified portions of a FOUO briefing are not required to be marked with a (U).

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Distribution Statement D: Distribution authorized to Department of Defense and U.S. DoD contractors only (reason) (date of determination).
Other requests for this document shall be referred to (controlling DARPA office).

Marking Applied for Training Purposes Only

IHMC Personnel

- Security / Facility Security Officer – Todd Norell
- Chief Information Officer – Alan Ordway
- Information System Security Manager – Fred Touchette

More Information

- DoD CUI Materials - <https://www.cdse.edu/toolkits/cui/index.php>
- CUI Webpage – <https://www.archives.gov/cui>
 - CUI Categories – <https://www.archives.gov/cui/registry/category-marking-list>
 - CUI Markings – <https://www.archives.gov/files/cui/20161206-cui-marking-handbook-v1-1.pdf>