Office of the Under Secretary of Defense for Intelligence and Security
OUSD (I&S)

Controlled Unclassified Information (CUI)

March 20, 2024

This briefing is UNCLASSIFIED. Markings are for training purposes only.

Definitions

Information Security (INFOSEC): policies, procedures, and requirements established in accordance with E.O. 13526, E.O. 13556, 32 CFR Part 2001, and 32 CFR Part 2002 to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to national security. **Encompasses classification, declassification, SCI, SAP, CUI.**

Executive Order 13526
32 CFR Part 2001
DoDI 5200.01
DoDM 5200.01 Volumes 1-3
DoDM 5200.45

Controlled Unclassified Information (CUI): information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a **law, regulation, or Government-wide policy** requires or permits an agency to handle using safeguarding or dissemination controls.

Executive Order 13556
32 CFR Part 2002
DoDI 5200.48

Operations Security (OPSEC): the process of **identifying critical information** and analyzing friendly actions attendant to military operations and other activities to: identify those actions that can be observed by adversary intelligence systems; determine indicators and vulnerabilities that adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries, and determine which of these represent an unacceptable risk; then select and execute countermeasures that eliminate the risk to friendly actions and operations or reduce it to an acceptable level.

NSPM-28
DoDD 5205.02E
DoDM 5205.02

Controlled Unclassified Information

Controlled Unclassified Information (CUI):

- Information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a **law, regulation, or Government-wide policy** requires or permits an agency to handle using safeguarding or dissemination controls.

Authorities
10 U.S.C. 130
15 CFR 772.1
15 CFR 774 Supplement 1
15 CFR 774 Supplement 2
22 CFR 120
22 CFR 121
48 CFR 252.204-7012

Applicable DoD Policies
DFARS 204.73
DoDD 5000.01
DoDD 5230.25
DoDI 2030.08
DoDI 2040.02
DoDI 3200.12
DoDI 5000.02
DoDI 5200.39

- Does not include classified information or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency.

- CUI is a control, not a classification.

DoDI 5200.48 Change 1

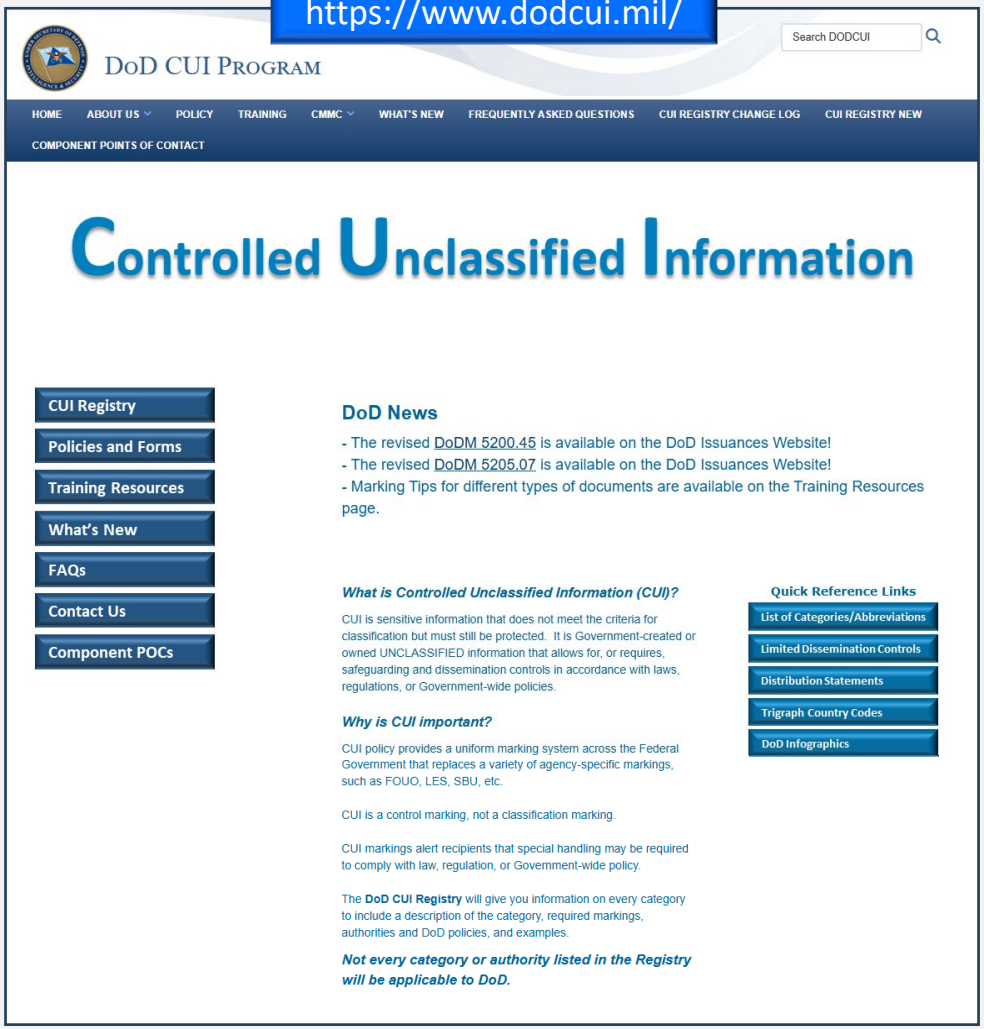
Currently in formal coordination.

Changes:

- Updates processes to clarify marking requirements, including the correct use of Not Releasable to Foreign Nationals (NOFORN) and Authorized for Release to (REL TO) markings.
- Eliminates reference to specified CUI.
- Eliminates the requirement for the CUI Warning Box on classified documents containing CUI.
- Adds requirements for tracking training completions and using the required DoD CUI training course.

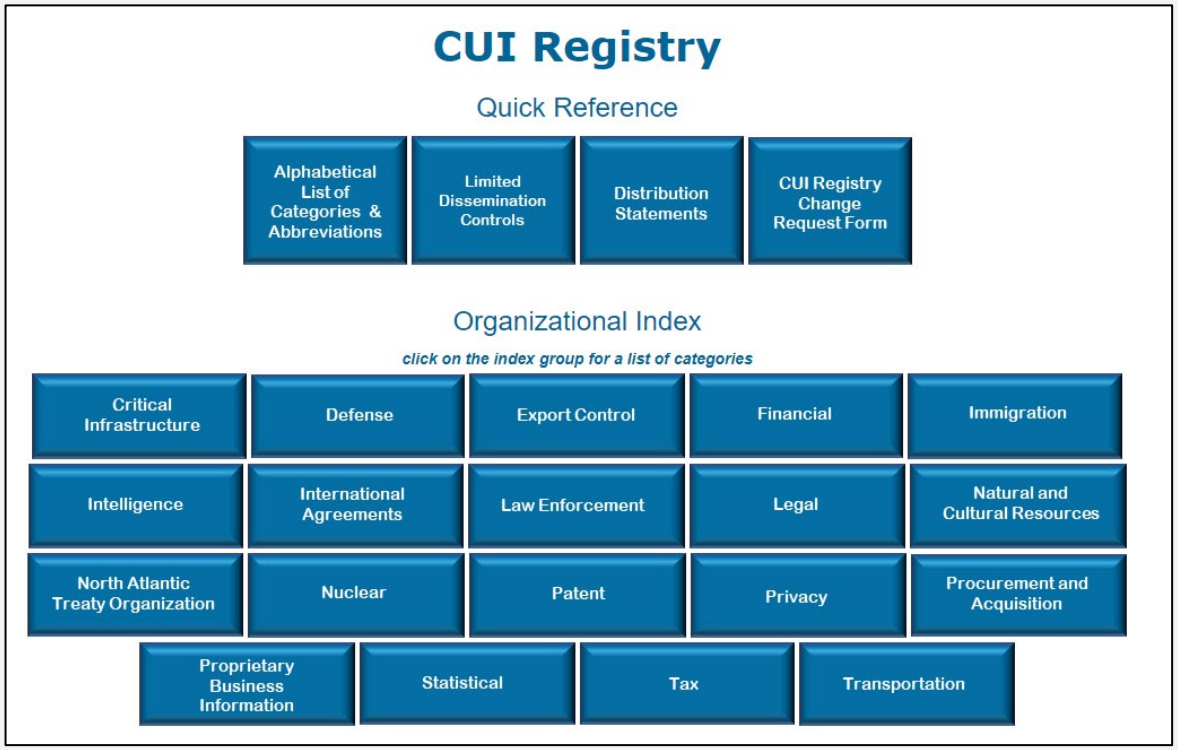
DoD CUI Website

https://www.dodcui.mil/



DoD CUI Registry

The key to correctly identifying unclassified information as CUI is ensuring it aligns with a CUI category in the DoD CUI Registry.



Defense Categories

- Controlled Technical Information
- DoD Critical Infrastructure Security Information
- Naval Nuclear Propulsion Information
- Privileged Safety Information
- Unclassified Controlled Nuclear Information - Defense

DoD CUI Registry

Each category has its own page and includes information about the category, examples of the type of information that falls in each category, authorities, and applicable DoD policies.

Controlled Technical Information

Back to Main Page

CUI Registry

Links to Defense Categories

DoD Critical Infrastructure Security Information
Naval Nuclear Propulsion Information
Privileged Safety Information
Unclassified Controlled Nuclear Information - Defense

Category Abbreviation:

CTI

Category Description:

Technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. The term does not include information that is lawfully publicly available without restrictions. "Technical Information" means technical data or computer software, as those terms are defined in Defense Federal Acquisition Regulation Supplement clause 252.227-7013, "Rights in Technical Data - Noncommercial Items" (48 CFR 252.227-7013).

Required Warning Statement:

Required Dissemination Control:

Distribution Statement B thru F

Examples

- Research and engineering data
- Engineering drawings
- Technical reports
- Technical data packages
- Design analysis
- Specifications
- Test reports
- Technical orders
- Cybersecurity plan
- IP addresses, nodes, links

Authorities

15 CFR 772.1
15 CFR 774 Supplement 1
15 CFR 774 Supplement 2
22 CFR 120
22 CFR 121
48 CFR 252.204-7012

Applicable DoD Policies

DFARS 204.73
DoDD 5000.01
DoDD 5230.25
DoDI 2030.08
DoDI 2040.02
DoDI 3200.12
DoDI 5000.02
DoDI 5200.39

Training Resources

DoD CUI Program

Search DODCUI

HOME | ABOUT US | POLICY | TRAINING | CMMC | WHAT'S NEW | FREQUENTLY ASKED QUESTIONS | CUI REGISTRY CHANGE LOG | CUI REGISTRY NEW | COMPONENT POINTS OF CONTACT

HOME > TRAINING

DoD Training

Training aids, references, infographics, CUI presentations, DoD Procurement Toolbox

Center for Development of Security Excellence (CDSE)

***CUI mandatory training course**; links to CDSE home page, security awareness hub, information security page, CUI toolkit, CUI shorts and webinars*

Information Security Oversight Office (ISOO)

Links to the ISOO CUI web page

Marking Tips

Markings are for training purposes only.

Banner Line	*CUI Designation Indicator Block*	*CUI in Classified Documents*	*Decontrol*
Distribution Statements	*Email*	*Limited Dissemination Controls*	*Maps and Photographs*
Portion Marking	*Slide Presentations*	*Spreadsheets*	*Technical Documents*
Web Pages	*Word Documents*		

CUI Marking Requirements

Marking Guidelines for Unclassified Documents Containing CUI

Mandatory CUI markings for unclassified documents include:

- The acronym "CUI" at the top and bottom of each page. 32 CFR Part 2002 gives agencies the option of marking documents with "CUI" or "CONTROLLED," but DoD only authorizes the use of "CUI."
- The CUI designation indicator block.

Do not add "UNCLASSIFIED" before "CUI."

Do not add the CUI category to the top and bottom of the page. The category is listed in the CUI designation indicator block.

✓CUI

✗U//CUI

✗CUI//OPSEC

✗CONTROLLED

Portion markings are optional, but recommended, on unclassified documents. If annotated, they must be applied to all portions, to include subjects, titles, paragraphs, subparagraphs, bullet points, figures, charts, tables, etc. Do not apply portion markings to the CUI designation indicator.

You are not required to place "CUI" in file names. The file or document name should be unclassified, so there is no requirement to mark it as CUI. If you want to indicate the document contains CUI, you can place a statement after the file name.

Example: Marking Requirements (Document is CUI)

The individual creating the document is responsible for applying the required markings.

CUI Marking Requirements

CUI Designation Indicator Block

The CUI designation indicator must be annotated on the first page or cover of all documents containing CUI.

Line 1: the name of the DoD Component and the office creating the document

Line 2: identification of the categories contained in the document

Line 3: applicable distribution statement or limited dissemination control (LDC)

Line 4: name and phone number or email of POC

Examples

Controlled by: OUSD(I&S)/DDI(CL&S)/IAP
CUI Category: NNPI
LDC: NOFORN
POC: John Brown, 703-555-0123

Controlled by: OUSD(I&S)/DDI(CL&S)/IAP
CUI Category: OPSEC
LDC: FEDCON
POC: osd.pentagon.rsrcmgmt.list.ousd-intel-infosec-mbx@mail.mil

Controlled by: OUSD(I&S)/DDI(CL&S)/IAP
CUI Category: CTI
Distribution Statement: C
POC: John Brown, 703-555-0123

Note: The distribution statement will be written out in full on the first page of the document as well as being annotated in the designation indicator block.

CUI Limited Dissemination Controls

Limited Dissemination Controls

LDCs are CUI executive agent-approved controls agencies may use to limit or specify CUI dissemination but cannot be used to unnecessarily restrict CUI access. Access to CUI should be encouraged and permitted to the extent that access or determination:

- Abides by the laws, regulations, or Government-wide policies that established the information as CUI.
- Furthers a lawful government purpose.
- Is not restricted by an authorized limited dissemination control established by the CUI executive agent.
- Is not otherwise prohibited by law.

LDCs establish additional control, secondary sharing, and release guidance without the need to repeatedly obtain controlling DoD office approval or authorization and identify the specific audience deemed to have a lawful government purpose to be an authorized holder of CUI.

The absence of an LDC on a document means anyone with a lawful government purpose is permitted access to the information but does not imply or authorize public release.

Control	Marking	Description
Federal Employees Only	FED ONLY	Dissemination authorized only to employees of the U.S. Government executive branch agencies or armed forces personnel of the U.S. or Active Guard and Reserve.
Federal Employees and Contractors Only	FEDCON	Includes individuals or employees who enter into a contract with the U.S. to perform a specific job, supply labor and materials, or for the sale of products and services, so long as dissemination is in furtherance of the contractual purpose.
No Dissemination to Contractors	NOCON	Intended for use when dissemination is not permitted to federal contractors, but permits dissemination to state, local, or tribal employees.
Dissemination List Controlled *	DL ONLY	Dissemination authorized only to those individuals, organizations, or entities included on an accompanying dissemination list.
Releasable by Information Disclosure Official	RELIDO	A permissive foreign disclosure and release marking used to indicate that the originator has authorized a Senior Foreign Disclosure and Release Authority (SFDRA) to make further sharing decisions for uncaveated intelligence material (intelligence with no restrictive dissemination controls) in accordance with existing procedures, guidelines, and implementation guidance. Note: Only agencies that are eligible to use RELIDO in the intelligence community (IC) classified information context may use this LDC on CUI. It is defined and applied in the same manner as in the IC context.
No Foreign Dissemination	NOFORN	Information may not be disseminated in any form to foreign governments, foreign nationals, foreign or international organizations, or non-U.S. citizens.
Authorized for Release to Certain Foreign Nationals Only	REL TO USA, [LIST]	Information has been predetermined by the designating agency to be releasable only to the foreign country(ies) or international organization(s) indicated, through established foreign disclosure procedures and channels. It is NOFORN to all foreign countries/international organizations not indicated in the REL TO marking. See list of approved country codes.
Display Only	DISPLAY ONLY	Information is authorized for disclosure to a foreign recipient, but without providing them a physical copy for retention to the foreign country(ies) or international organization(s) indicated, through established foreign disclosure procedures and channels.
Attorney Client	ATTORNEY-CLIENT	Dissemination of information beyond the attorney, the attorney's agents, or the client is prohibited, unless the agency's executive decision makers decide to disclose the information outside the bounds of its protection.
Attorney Work Product	ATTORNEY-WP	Dissemination of information beyond the attorney, the attorney's agents, or the client is prohibited, unless specifically permitted by the overseeing attorney who originated the work product or their successor.

* DL ONLY is used when you have a specific organization or list of individuals authorized to receive the document and none of the other LDCs apply. The list must be on or attached to the document, or a link to the list annotated on the document.

Distribution Statements

Distribution statements, in accordance with DoDI 5230.24, are authorized for use with:

- CUI export controlled information
- Controlled technical information
- Other scientific, technical, and engineering information

Distribution Statement A: Approved for public release. Distribution is unlimited.

Distribution Statement B: Distribution authorized to U.S. Government agencies only [fill in reason and date of determination].

Distribution Statement C: Distribution authorized to U.S. Government agencies and their contractors [fill in reason and date of determination]. Other requests for this document shall be referred to [insert controlling DoD office].

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

Distribution Statement E: Distribution authorized to DoD Components only [fill in reason and date of determination]. Other requests shall be referred to [insert controlling DoD office].

Distribution Statement F: Further dissemination only as directed by [insert controlling DoD Office and date of determination] or higher DoD authority.

Note: A distribution statement does not automatically mean the document contains CUI. Certain types of CUI require a distribution statement, but distribution statements can be applied to all technical and scientific information.

Safeguarding and Storage Requirements

- DoD personnel must keep CUI under their control at all times or protect it with at least one physical barrier to reasonably ensure the CUI is protected from unauthorized access and observation. Acceptable methods include using the SF 901 cover sheet, turning computer monitors off, or using monitor screen covers.
- Use the SF 710 Unclassified Label to mark media and peripheral equipment.
- During duty hours, CUI storage options include locked or unlocked containers, desk drawers, or GSA-approved storage cabinets.
- After duty hours:
  - Unlocked containers, desks, or cabinets if the building provides continuous monitoring (e.g., 24-hour security guards, intrusion detection system).
  - Locked desks, file cabinets, bookcases, locked rooms, or similarly secured areas if the building does not provide continuous monitoring.
- Locked desks, file cabinets, bookcases, or similarly secured areas in hotel rooms or other temporary lodgings can be used.
- Do not store CUI in automobiles.
- Do not view CUI while on public transportation.

If you believe there has been a spillage or unauthorized disclosure of CUI, report it to your supervisor or security manager.

Destruction Requirements

- Documents containing CUI may be destroyed using the same methods as for classified information.
- CUI must be made unreadable, indecipherable, and irrecoverable once destroyed. Materials containing CUI will be destroyed using paper, optical media, or other destruction devices listed on the current National Security Agency Evaluated Products List, available at https://www.nsa.gov/Resources/Media-Destruction-Guidance/.
- Use cross-cut shredders that produce 1 mm x 5 mm (0.04 inch x 0.2 inch) or smaller particles.
- Pulverize or disintegrate paper using disintegrator devices equipped with a 3/32 inch (2.4 mm) security screen.
- Dispose of CUI using any other destruction methods LRGWPs specifically require.
- Authorized CUI holders may consolidate CUI prior to shredding, recycling, or destroying it, including shred bins and burn bags within the organization's controlled environments and interim storage or contractor facilities.

CUI Markings

Action/Info Memo

Required Markings:
- Banner line, top and bottom
- CUI designation indicator block

Optional:
- Portion markings

Without portion marks

Banner Line → CUI

ACTION MEMO

FOR: SECRETARY OF DEFENSE DepSecDef Action _____

FROM: Ronald S. Moultrie, Under Secretary of Defense for Intelligence & Security

SUBJECT: Delegation of Original Classification Authority

- **Purpose.** Request the Secretary of Defense (SecDef) approve the delegation of Top Secret (TS) original classification authority (OCA) to the Director for Defense Intelligence (Counterintelligence, Law Enforcement, & Security) (DDI(CL&S)).
- **Background.** Executive Order (E.O.) 13526, "Classified National Security Information," establishes the requirements for delegating OCA authority and provides that TS OCA may be delegated only by the President, the Vice President, or an appropriated designated agency head or official, such as the SecDef. E.O. 13526 requires delegations of OCA to be in writing, and the officials to be identified by position, and that all OCAs receive training in proper classification and declassification at least once a year.
- DoD Manual (DoDM) 5200.01, Volume 1, "DoD Information Security Program: Overview, Classification, and Declassification," further limits delegation of OCA to instances when:
  1. There is a demonstrable and continuing need to exercise OCA during the normal course of operations;
  2. Such demonstrable and continuing need cannot be met through issuance of security classification guides by existing OCAs in the chain of command;
  3. Referral of decisions to existing OCAs at higher levels in the chain of command or supervision is not practical for reasons such as geographical separation; and
  4. Sufficient expertise and information is available to the prospective OCA to permit effective classification decision-making.
- I have concluded that the requirements in E.O. 13526 and DoDM 5200.01, Volume 1 have been met. Further, this request is consistent with TS OCA granted to other Defense Components and Agencies.

RECOMMENDATION: Sign Memorandum at TAB B.

Attachments:
TAB B – SecDef Memo to DDI(CL&S)
TAB C – Coordination

CUI Designation Indicator Block

Controlled by: DDI(CL&S)/IAP
CUI Category: PSI
LDC: FEDCON
POC: osd.pentagon.rsrcmgmt.list.ousd-intel-infosec-mbx@mail.mil

Banner Line → CUI

Markings are for training purposes only.

CUI Markings

Action/Info Memo

Required Markings:
- Banner line, top and bottom
- CUI designation indicator block

Optional:
- Portion markings

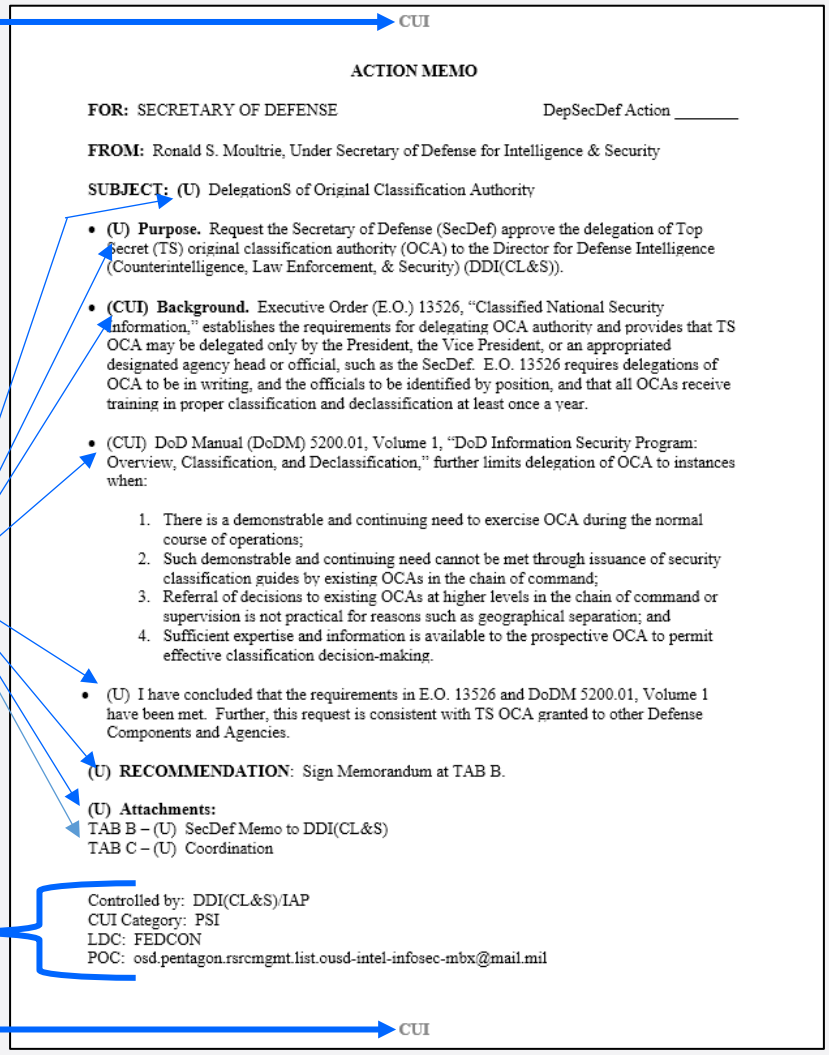
With portion marks

Banner Line

Portion marks

CUI Designation Indicator Block

Banner Line



CUI

ACTION MEMO

FOR: SECRETARY OF DEFENSE DepSecDef Action _____

FROM: Ronald S. Moultrie, Under Secretary of Defense for Intelligence & Security

SUBJECT: **(U)** DelegationS of Original Classification Authority

- **(U) Purpose.** Request the Secretary of Defense (SecDef) approve the delegation of Top Secret (TS) original classification authority (OCA) to the Director for Defense Intelligence (Counterintelligence, Law Enforcement, & Security) (DDI(CL&S)).
- **(CUI) Background.** Executive Order (E.O.) 13526, "Classified National Security Information," establishes the requirements for delegating OCA authority and provides that TS OCA may be delegated only by the President, the Vice President, or an appropriated designated agency head or official, such as the SecDef. E.O. 13526 requires delegations of OCA to be in writing, and the officials to be identified by position, and that all OCAs receive training in proper classification and declassification at least once a year.
- (CUI) DoD Manual (DoDM) 5200.01, Volume 1, "DoD Information Security Program: Overview, Classification, and Declassification," further limits delegation of OCA to instances when:
  1. There is a demonstrable and continuing need to exercise OCA during the normal course of operations;
  2. Such demonstrable and continuing need cannot be met through issuance of security classification guides by existing OCAs in the chain of command;
  3. Referral of decisions to existing OCAs at higher levels in the chain of command or supervision is not practical for reasons such as geographical separation; and
  4. Sufficient expertise and information is available to the prospective OCA to permit effective classification decision-making.
- (U) I have concluded that the requirements in E.O. 13526 and DoDM 5200.01, Volume 1 have been met. Further, this request is consistent with TS OCA granted to other Defense Components and Agencies.

(U) RECOMMENDATION: Sign Memorandum at TAB B.

(U) Attachments:
TAB B – (U) SecDef Memo to DDI(CL&S)
TAB C – (U) Coordination

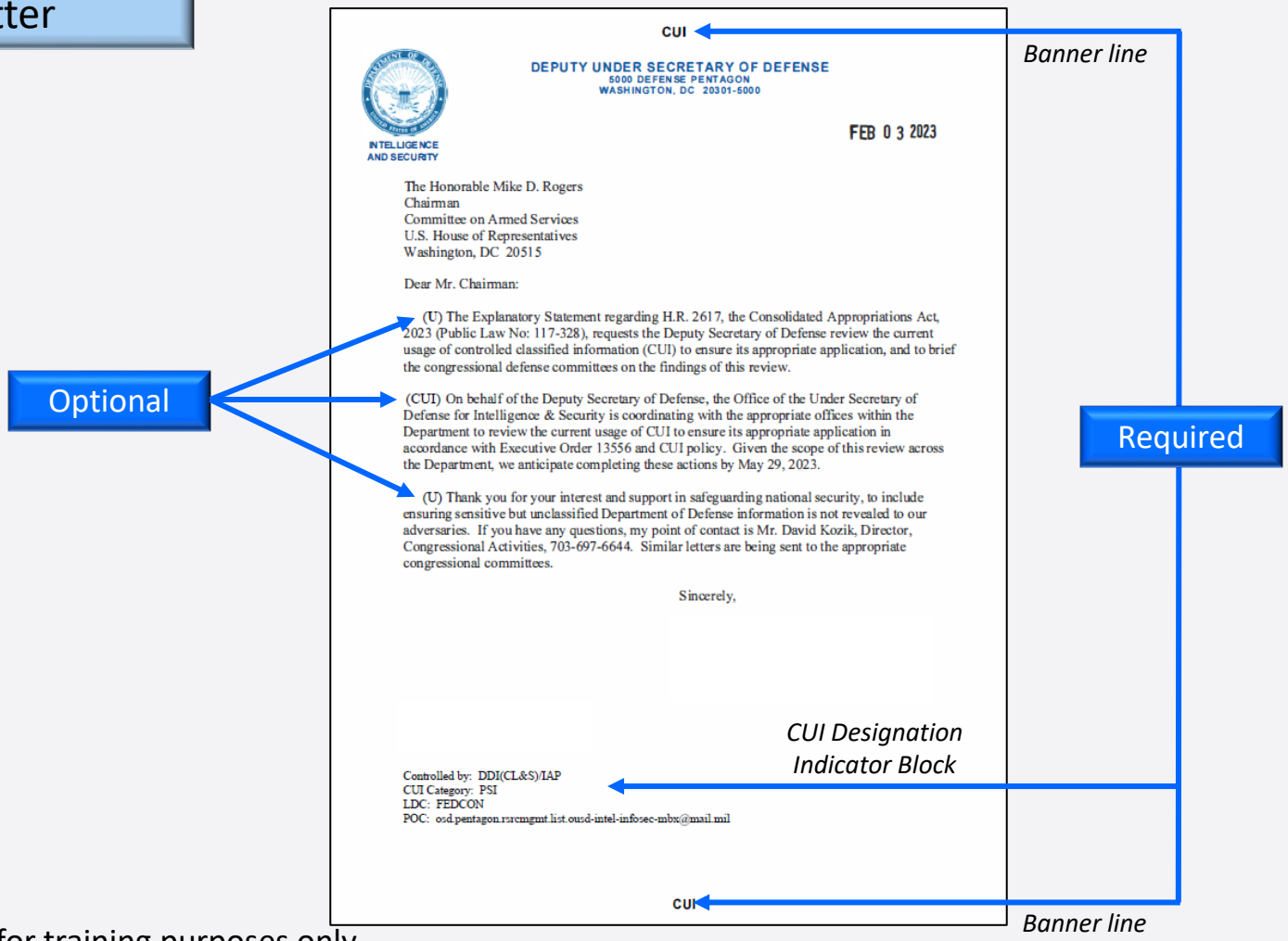
Controlled by: DDI(CL&S)/IAP
CUI Category: PSI
LDC: FEDCON
POC: osd.pentagon.rsrcmgmt.list.ousd-intel-infosec-mbx@mail.mil

CUI

Markings are for training purposes only.

CUI Markings

Letter



Markings are for training purposes only.

CUI Markings

Markings are for training purposes only.

Memo

CUI

UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

SEP 2 7 2023

INTELLIGENCE AND SECURITY

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP
COMMANDERS OF THE COMBATANT COMMANDS
DEFENSE AGENCY AND DOD FIELD ACTIVITY DIRECTORS

SUBJECT: Use of Digital Signatures on Standard Form 312

References: (a) Executive Order 13526, "Classified National Security Information," January 5, 2010
(b) 32 Code of Federal Regulations, Part 2001, June 28, 2010
(c) ISOO Notice 2022-01: "Digital Signatures on Standard Form (SF) 312, Classified Information Nondisclosure Agreement," May 9, 2022
(d) DoD Manual 5200.01, Volume 1, "DoD Information Security Program: Overview, Classification, and Declassification," February 24, 2012, as amended

The Information Security Oversight Office, as Executive Agent for references (a) and (b), issued updated guidance to Departments and Agencies on the use of digital signatures on Standard Form (SF) 312, "Classified Information Non-Disclosure Agreement" at reference (c). Based upon that guidance and in the interest of information security reform, Department of Defense (DoD) Components are authorized to accept digital signatures on all SF 312s as described in this memorandum.

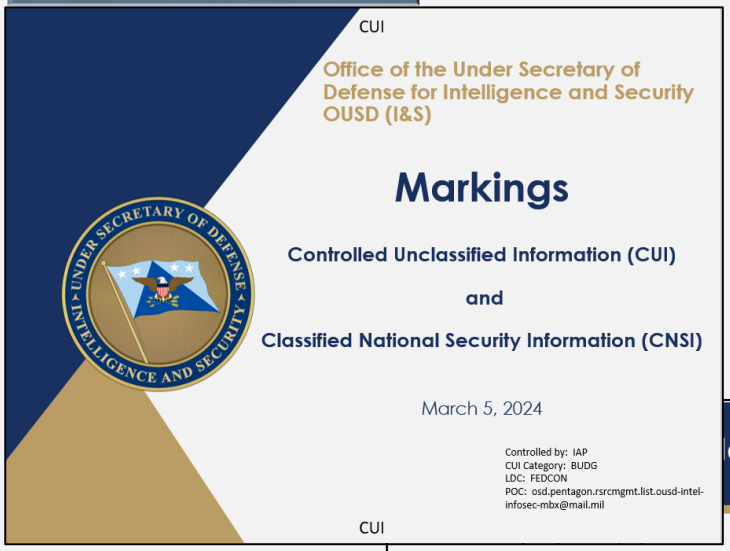
DoD military, civilian, and contractor personnel may now sign SF 312s using a DoD-issued credential that is: (1) based on public key infrastructure (PKI) and (2) includes a reliable certificate authority (CA). This includes the common access card, DoD-approved derived credentials (e.g., Purebred), personal identity verification (PIV), or DoD-approved PIV-Interoperable (PIV-I) cards. In addition, DoD personnel may use digital signatures from DoD-sponsored External Certificate Authority PKIs, which are listed at https://cyber.mil/eca/, and DoD-approved external PKIs, which are listed at https://cyber.mil/pki-pke/interoperability/. DoD-approved external PKIs include certain federal personal PIV and industry PIV-I PKI credentials.

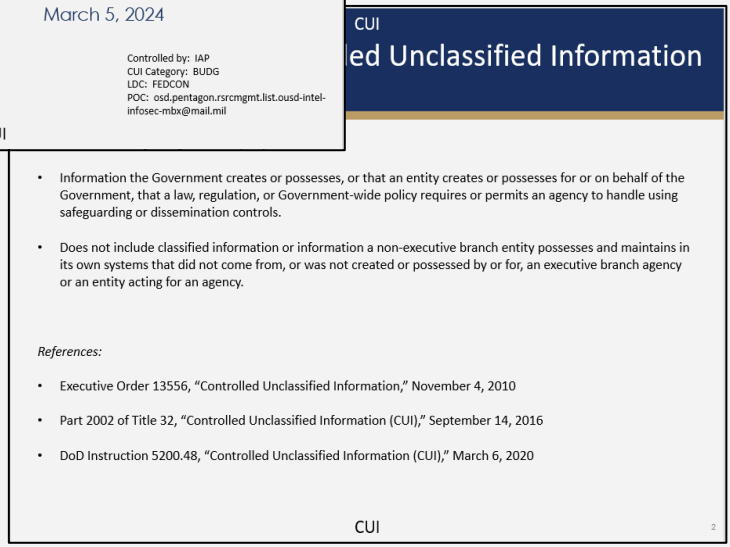
DoD components will reciprocally accept SF 312s containing digital or manual signatures, or a combination of both. Because of the authentication, consent, and integrity provided by the digital signature, the witness block does not require a signature if the user signs digitally. However, a digital or manual signature in the Acceptance block is still required.

Controlled by: Mark Brown, Analyst
CUI Category: PSI
LDC: FEDCON
POC: 703-555-9654

CUI

PowerPoint



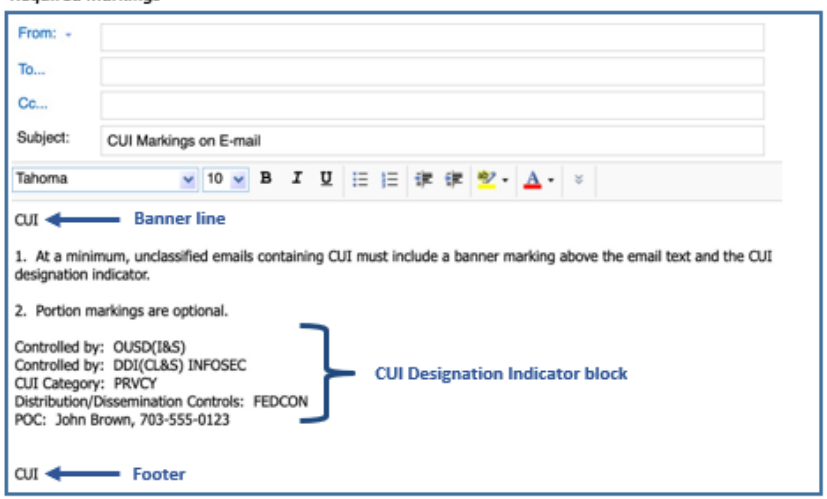


CUI Markings

Email

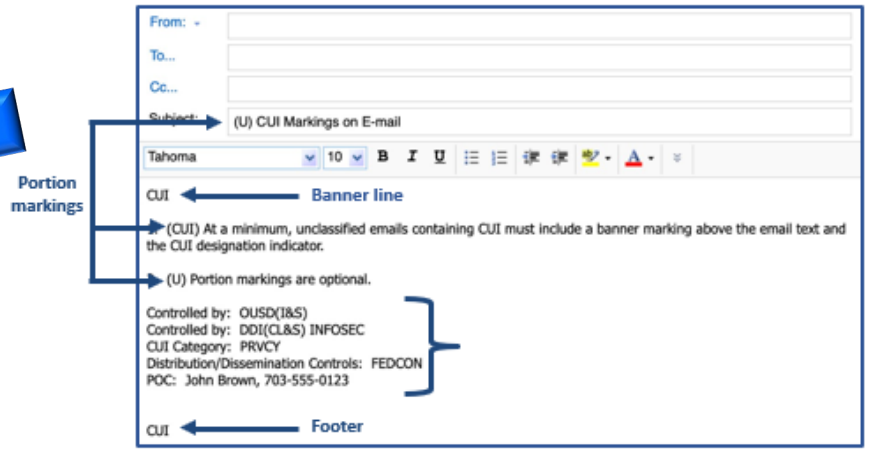
Without portion marks

Required markings



With portion marks

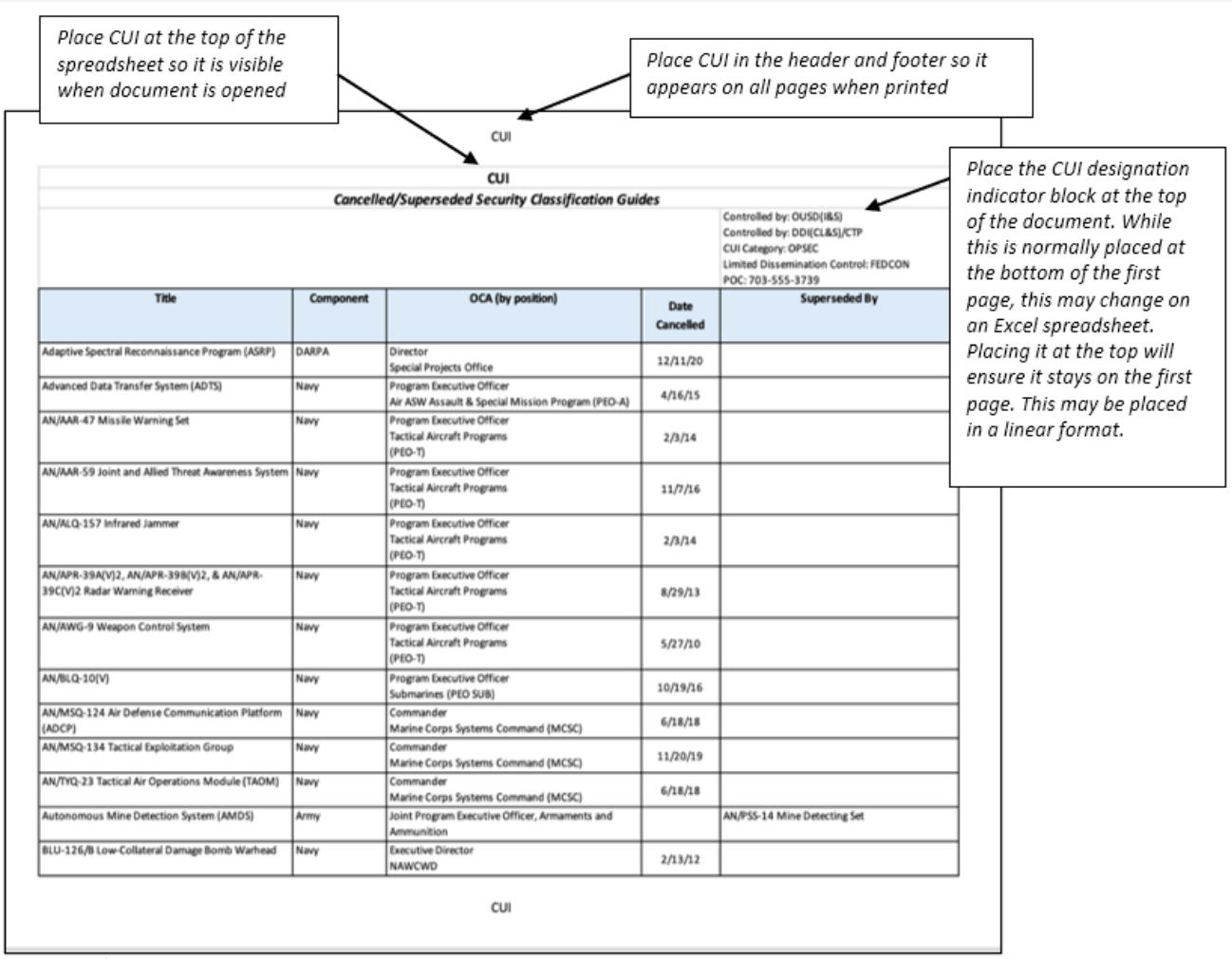
Portion markings included



Markings are for training purposes only.

CUI Markings

Excel



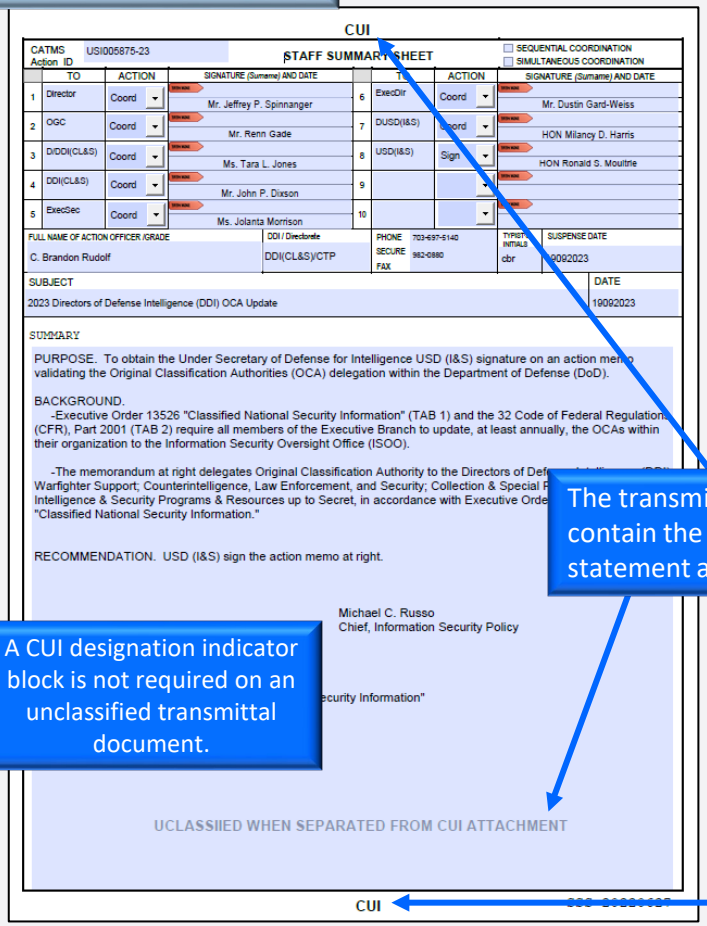
Title	Component	OCA (by position)	Date Cancelled	Superseded By
Adaptive Spectral Reconnaissance Program (ASRP)	DARPA	Director Special Projects Office	12/11/20	
Advanced Data Transfer System (ADTS)	Navy	Program Executive Officer Air ASW Assault & Special Mission Program (PEO-A)	4/16/15	
AN/AAR-47 Missile Warning Set	Navy	Program Executive Officer Tactical Aircraft Programs (PEO-T)	2/3/14	
AN/AAR-59 Joint and Allied Threat Awareness System	Navy	Program Executive Officer Tactical Aircraft Programs (PEO-T)	11/7/16	
AN/ALQ-157 Infrared Jammer	Navy	Program Executive Officer Tactical Aircraft Programs (PEO-T)	2/3/14	
AN/APR-39A(V)2, AN/APR-39B(V)2, & AN/APR-39C(V)2 Radar Warning Receiver	Navy	Program Executive Officer Tactical Aircraft Programs (PEO-T)	8/29/13	
AN/AWG-9 Weapon Control System	Navy	Program Executive Officer Tactical Aircraft Programs (PEO-T)	5/27/10	
AN/BLQ-10(V)	Navy	Program Executive Officer Submarines (PEO SUB)	10/19/16	
AN/MSQ-124 Air Defense Communication Platform (ADCP)	Navy	Commander Marine Corps Systems Command (MCSC)	6/18/18	
AN/MSQ-134 Tactical Exploitation Group	Navy	Commander Marine Corps Systems Command (MCSC)	11/20/19	
AN/TYQ-23 Tactical Air Operations Module (TAOM)	Navy	Commander Marine Corps Systems Command (MCSC)	6/18/18	
Autonomous Mine Detection System (AMDS)	Army	Joint Program Executive Officer, Armaments and Ammunition		AN/PSS-14 Mine Detecting Set
BLU-126/B Low-Collateral Damage Bomb Warhead	Navy	Executive Director NAWCWD	2/13/12	

Markings are for training purposes only.

CUI Markings

Markings are for training purposes only.

Transmittal Document



CUI

CATMS Action ID: USI005875-23

STAFF SUMMARY SHEET

☐ SEQUENTIAL COORDINATION
☐ SIMULTANEOUS COORDINATION

	TO	ACTION	SIGNATURE (Surname) AND DATE		TO	ACTION	SIGNATURE (Surname) AND DATE
1	Director	Coord	Mr. Jeffrey P. Spinnanger	6	ExecDir	Coord	Mr. Dustin Gard-Weiss
2	OGC	Coord	Mr. Renn Gade	7	DUSD(I&S)	Coord	HON Milancy D. Harris
3	DDDI(CL&S)	Coord	Ms. Tara L. Jones	8	USD(I&S)	Sign	HON Ronald S. Moultrie
4	DDI(CL&S)	Coord	Mr. John P. Dixson	9			
5	ExecSec	Coord	Ms. Jolanta Morrison	10			

FULL NAME OF ACTION OFFICER /GRADE	DDI / Directorate	PHONE 703-697-5140	TYPIST INITIALS	SUSPENSE DATE
C. Brandon Rudolf	DDI(CL&S)/CTP	SECURE 962-0980 FAX	cbr	19092023

SUBJECT: 2023 Directors of Defense Intelligence (DDI) OCA Update — DATE: 19092023

SUMMARY

PURPOSE. To obtain the Under Secretary of Defense for Intelligence USD (I&S) signature on an action memo validating the Original Classification Authorities (OCA) delegation within the Department of Defense (DoD).

BACKGROUND.
-Executive Order 13526 "Classified National Security Information" (TAB 1) and the 32 Code of Federal Regulations (CFR), Part 2001 (TAB 2) require all members of the Executive Branch to update, at least annually, the OCAs within their organization to the Information Security Oversight Office (ISOO).

-The memorandum at right delegates Original Classification Authority to the Directors of Def... Warfighter Support; Counterintelligence, Law Enforcement, and Security; Collection & Special P... Intelligence & Security Programs & Resources up to Secret, in accordance with Executive Orde... "Classified National Security Information."

RECOMMENDATION. USD (I&S) sign the action memo at right.

Michael C. Russo
Chief, Information Security Policy

...ecurity Information"

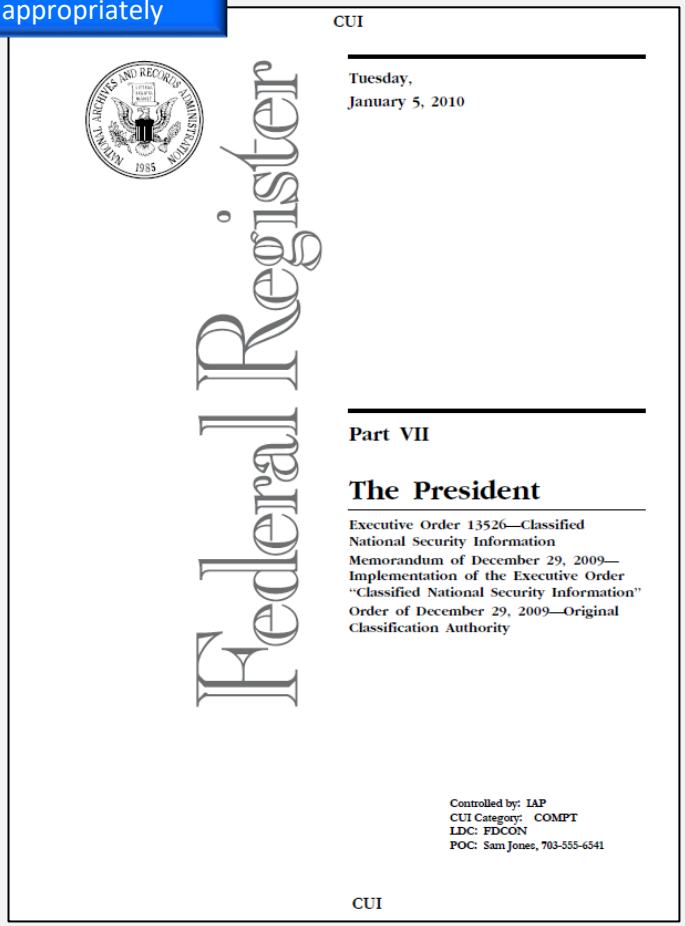
UCLASSIIED WHEN SEPARATED FROM CUI ATTACHMENT

CUI

The attachment will be marked appropriately

The transmittal document will contain the banner line and a statement at the bottom

A CUI designation indicator block is not required on an unclassified transmittal document.



CUI

Federal Register

Tuesday,
January 5, 2010

Part VII

The President

Executive Order 13526—Classified National Security Information

Memorandum of December 29, 2009—Implementation of the Executive Order "Classified National Security Information"

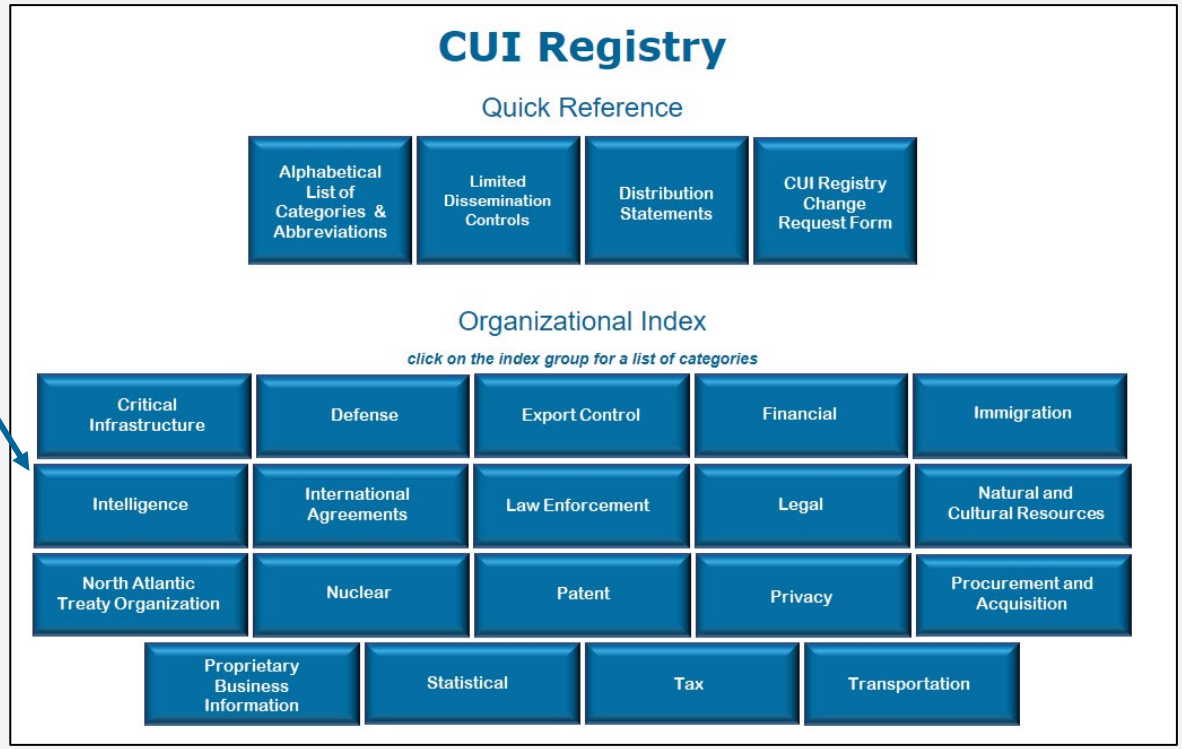
Order of December 29, 2009—Original Classification Authority

Controlled by: IAP
CUI Category: COMPT
LDC: FDCON
POC: Sam Jones, 703-555-6541

CUI

OPSEC

The OPSEC CUI category is under Intelligence.



OPSEC

Operations Security

Back to Main Page

CUI Registry

Categories and Abbreviations

Links to Intelligence Categories

Agriculture
Foreign Intelligence Surveillance Act
FISA Business Records
General Intelligence
Geodetic Product Information
Intelligence Financial Records
Internal Data

Category Abbreviation:

OPSEC

Category Description:

Critical information determined to give evidence of the planning and execution of sensitive (frequently classified) government activities after going through a formal systematic vetting process in accordance with National Security Presidential Memorandum Number 28. This process identifies unclassified information that must be protected. It almost always results from an agency's official OPSEC program, or is otherwise commonly approved for use by the CUI Senior Agency Official.

NOTE: Information on your organization's Critical Information List (CIL) MAY BE CUI. It depends on what information is included in your document and how it is stated. To use the OPSEC category, the information must be on the CIL.

Required Warning Statement:

Required Dissemination Control:

Examples

- Critical Information List (CIL)
- OPSEC planning
- Risk assessment plan
- Security classification guides

Authorities

NSPM-28 (contact your OPSEC office for a copy)

Applicable DoD Policies

DoDD 5205.02E
DoDM 5205.02

Unauthorized Disclosures

A UD occurs when unauthorized individuals gain access to CUI through physical, auditory, or electronic means.

CUI mishandling occurs when an authorized CUI holder fails to employ required CUI controls, regardless of whether a UD resulted.

Because all CUI is associated with an LRGWP, individual consequences for safeguarding and handling violations can extend beyond administrative penalties to civil and criminal proceedings.

The DoD Components' senior agency officials (CSAO) and Component Program Managers (CPM) will establish procedures to ensure prompt and appropriate management action is taken in cases of CUI misuse, including UD of CUI, improper CUI designation and marking, violation of this issuance, and incidents potentially placing CUI at risk of UD. Such actions will focus on correcting or eliminating the conditions contributing to the incident.

DoD personnel are required to report:

(1) Any actual or suspected mishandling of CUI.

(2) Any suspicious behaviors among the workforce with potential to compromise CUI.

No formal security inquiry or investigation is required unless disciplinary action will be taken against the individual(s) responsible. UD of certain CUI, such as export controlled-technical data, may also result in potential civil and criminal sanctions against responsible persons based on the procedures codified in the relevant LRGWP. The DoD Component originating the CUI will be informed of any UD.

Incidents involving the UD of CUI will be reported through command channels to the DCSA DoD Insider Threat Management and Analysis Center. The Insider Threat Management and Analysis Center manages the Unauthorized Disclosure Program Management Office and serves as the central DoD office for consistent, uniform, and timely reporting of UDs.

Lessons Learned

OPSEC is not the default CUI category.

In the early days, it seemed everyone would use OPSEC because it was easy. This led to improved instructions on the CUI website.

Users must look at the information revealed to determine the correct category.

Security classification guides may be protected as CUI under the OPSEC category.

Contact Information

INFOSEC Mailboxes:

NIPR: osd.pentagon.rsrcmgmt.list.ousd-intel-infosec-mbx@mail.mil

SIPR: osd.pentagon.rsrcmgmt.list.ousd-intel-infosec-mbx@mail.smil.mil

CUI Web Page: https://www.dodcui.mil