



**NATIONAL GUARD BUREAU**  
1636 DEFENSE PENTAGON  
WASHINGTON DC 20301-1636

CNGB DTM 2401.00  
NGB-J2  
09 September 2025

MEMORANDUM FOR NATIONAL GUARD BUREAU

Subject: Controlled Unclassified Information in National Guard Bureau Email Correspondence

References: See Attachment J.

1. Purpose. This Chief of the National Guard Bureau (CNGB) Directive Type-Memorandum (DTM) establishes interim policy and procedures for Controlled Unclassified Information (CUI) in accordance with the references.
2. Cancellation. None.
3. Applicability. This CNGB DTM applies to all National Guard Bureau (NGB) personnel.
4. Policy. It is NGB policy to correctly handle CUI through the proper designation, marking, protection, and dissemination for mitigating unauthorized disclosures. All personnel are considered CUI Custodians for proper CUI handling. All email correspondence, including attachments, must be accurately marked to protect sensitive unclassified information. Properly marking emails to distinguish between CUI and Unclassified, per the guidance in reference b, is essential. This includes portion marking each line and paragraph in the body of every correspondence. This process safeguards sensitive data while allowing appropriate public release, thereby maintaining necessary security controls and enhancing transparency.
  - a. NGB Personnel. All NGB personnel must verify whether an email contains CUI data by consulting the CUI Registry and adhering to the CUI marking policy. Emails with CUI must include "CUI" in the subject line, have a "CUI" marking in the relevant paragraphs, label any attachments with "CUI" in the filename, and feature a CUI disclaimer and designation block. All emails containing CUI will be encrypted. Refer to Attachment E for further guidance.
  - b. Determination. Only the originator can determine if information is CUI. To determine if the information requires specific safeguarding and dissemination controls, the information originator will review the CUI Registry at reference a, and Attachment C to decide what category, or categories, the information falls within. If the information does not align with any category, it cannot be marked CUI. Refer to Attachment B for determination assistance.

c. Dissemination. Only the originator can set controls for disseminating CUI. Once confirmed that the information qualifies as CUI, the originator must establish the dissemination controls. These controls may indicate that distribution is either limited or prohibited. CUI Custodians and originators can review the dissemination control list and each definition in reference a, and Attachment D.

d. Markings. When drafting official correspondence and handling CUI, the CUI Custodians must identify the category or categories in which the information falls using reference a, and Attachment C (for example, PRVCY and OPSEC), and apply the appropriate control markings. This may be completed manually or by using Microsoft tools depending on your operating system or recent patch update (see Attachment E and Attachment F).

(1) Email Correspondence. All email correspondence containing CUI will be encrypted. In addition to encryption, emails containing CUI will include the following markings: "CUI" in the subject line, have a "CUI" marking in the relevant paragraphs, label any attachments with "CUI" in the filename, and feature a CUI designation block. Refer to Attachment E for the email CUI Marking Guide and reference e for detailed instructions. It is up to the individual CUI Custodian to properly mark CUI. This can be done manually with the assistance of the DoD CUI Registry or through automated marking tools, depending on their information system marking tools. For most Outlook users, an embedded CUI labeling tool is located on the right side of the "Subject" line of a new email correspondence; see Attachment E (Outlook CUI Labeling Tool) for tool use and functional capabilities.

(2) Microsoft Word and Portable Document Format. In accordance with reference e, all documents containing CUI will have the following markings:

- (a) CUI indicated in the header and footer.
- (b) Portion markings before the subject title if it includes CUI, as well as at the start of each title and paragraph containing CUI.
- (c) CUI portion markings to relevant headings, images, graphs, charts, maps, and reference lists.
- (d) CUI Designation Indicator Block in the footer of the document without a portion mark. Refer to Attachment E for the Document CUI Marking Guide.

(3) PowerPoint. All PowerPoint products containing CUI must have the following markings: "CUI" in the header and footer banner, CUI portion markings at the beginning of separate sentences and paragraphs, and a CUI Designation Indicator Block on the first slide. Refer to Attachment H for the PowerPoint CUI Marking Guide.

(4) Microsoft Teams. When sending CUI using Microsoft Teams chat, each CUI sentence and paragraph will have a CUI portion marking. Documents saved in Microsoft Teams will have "CUI" at the beginning of the file name.

e. Unmarked or Mismarked Information. If you encounter information that appears to be CUI and lacks appropriate markings, you should treat it as CUI until you can confirm its status with the originator. If information is, in fact, CUI, the originator will apply applicable markings and transmission adherence.

f. Unauthorized Disclosure. In case of an unauthorized disclosure, report it immediately to the directorate Security Assistant where the unauthorized disclosure occurred, and the National Guard Bureau Joint Intelligence Directorate (NGB-J2) Counterintelligence and Security Division (NGB-J24). Secure any compromised information, if possible. Document the incident, identify the source, and take corrective action in accordance with reference d, to prevent future occurrences.

g. Training Requirements. Refresher and scenario-focused training for staff is available from NGB-J24 by request. This training does not replace individual computer-based training requirements. All NGB personnel, including contractors, must complete the training in Attachment A.

5. Responsibilities. See Attachment A.

6. Coordination and Resources.

a. Virtual Monthly Touchpoints. The appointed Security Assistants will attend monthly virtual touchpoints to receive training and policy updates and review security vignettes to ensure directorates are on track with annual requirements before the annual Information Security Oversight Office self-inspection.

b. NGB Joint Staff Security Assistant Microsoft Teams Page (Teams Page: NGB Joint Staff Security Assistants). The Security Assistants will ensure access and monitor the NGB Joint Staff Security Assistant Microsoft Teams page for the most current information and correspondence.

c. Point of Contact. The point of contact for all CUI inquiries is the NGB-J24 Information Security Branch, NGB-J24, at the following group mailbox: National Guard National Capital Region NGB Army National Guard mailbox NGB-J24 Information Security (INFOSEC) <ng.ncr.ngb-arng.mbx.ngb-j24-infosec@army.mil>, or by calling 703-601-7359.

7. Information Collection Requirements. Each directorate will be required to submit 15 CUI documents to the NGB-J24 INFOSEC email <ng.ncr.ngb-arng.mbx.ngb-j24-infosec@army.mil>. The document submissions will be assessed for marking accuracy and compliance of the DoD CUI Program. NGB-J24 is required to submit findings and compliance and training metrics to the Information Security Oversight Office.

8. Definitions. See Glossary.

9. Releasability. This CNGB DTM is approved for public release; distribution is unlimited. It is available at <<https://www.ngbpmc.ng.mil/>>.

10. Records Management. This CNGB DTM and all records created as a result, regardless of media and format, must be managed in accordance with the NGB Records Management Program.

11. Compliance. Per the CNGB 5000.01 Issuance Series, the proponent will review this CNGB DTM annually on the anniversary of its effective date to either confirm the action has been completed, incorporate the directive into an CNGB Issuance, or to update and extend the CNGB DTM's continued applicability, validity, and consistency with Federal, Department of Defense, and NGB policy and provide validation to the Strategy, Policy, Plans, and International Affairs Directorate and the NGB Executive Secretariat Issuances Branch.

A handwritten signature in black ink, appearing to read "St. S. Nordhaus", with a stylized, flowing script.

STEVEN S. NORDHAUS  
General, USAF  
Chief, National Guard Bureau

Attachments:  
As stated

ATTACHMENT A  
RESPONSIBILITIES

1. NGB-J24. NGB-J24 implements all security-related programs on behalf of the NGB-J2 and the NGB Director of Staff.

a. Provide up-to-date statutory and regulatory guidance to the NGB Joint Staff Directorate Security Assistants.

b. Confirm receipt of all Security Assistant appointment memorandums and validate staff training compliance.

c. Provide guidance and assistance, as necessary, to the Security Assistants.

d. Host monthly virtual Security Assistant touchpoints using Microsoft Teams.

2. Appointed Security Assistants. The appointed Security Assistants will:

a. Implement all security-related policy and procedures within their directorate.

b. Provide internal training and compliance oversight.

c. Ensure personnel are properly trained and training records are recorded.

3. All Personnel.

a. CUI Training. All personnel, including contractors, must complete annual CUI training. Reference b directs all personnel to receive initial and annual refresher training. The training is found on the Center for Development of Security Excellence (CDSE) website, Course IF141.06 (see reference k).

b. INFOSEC. All personnel, including contractors, must complete annual INFOSEC training. Reference f, Attachment I, and reference b direct all personnel to receive initial and annual refresher training. The training is found on the CDSE website, Course IF142.06 (see reference h.)

c. Personally Identifiable Information. All personnel, including contractors, must complete annual Personally Identifiable Information training. Reference a directs initial and annual refresher training. The training is found on the CDSE website, Course DS-IF101.06 (see reference k).

4. Select Personnel. Select Personnel will complete derivative classification training before a Secret Internet Protocol Router token application is approved. Training is found on the CDSE website, Course IF103.16, (see reference k).

ATTACHMENT B

CONTROLLED UNCLASSIFIED INFORMATION DETERMINATION

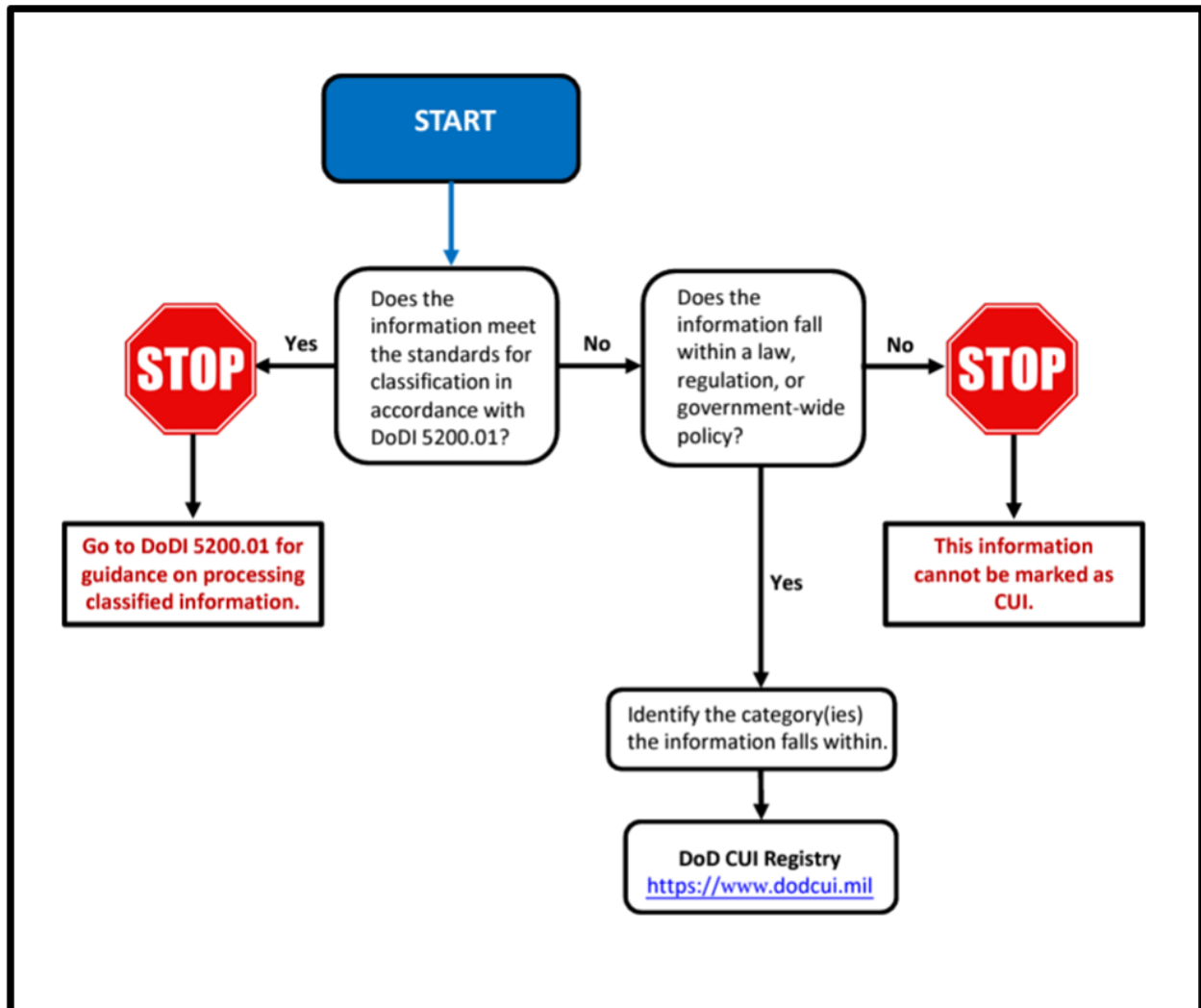
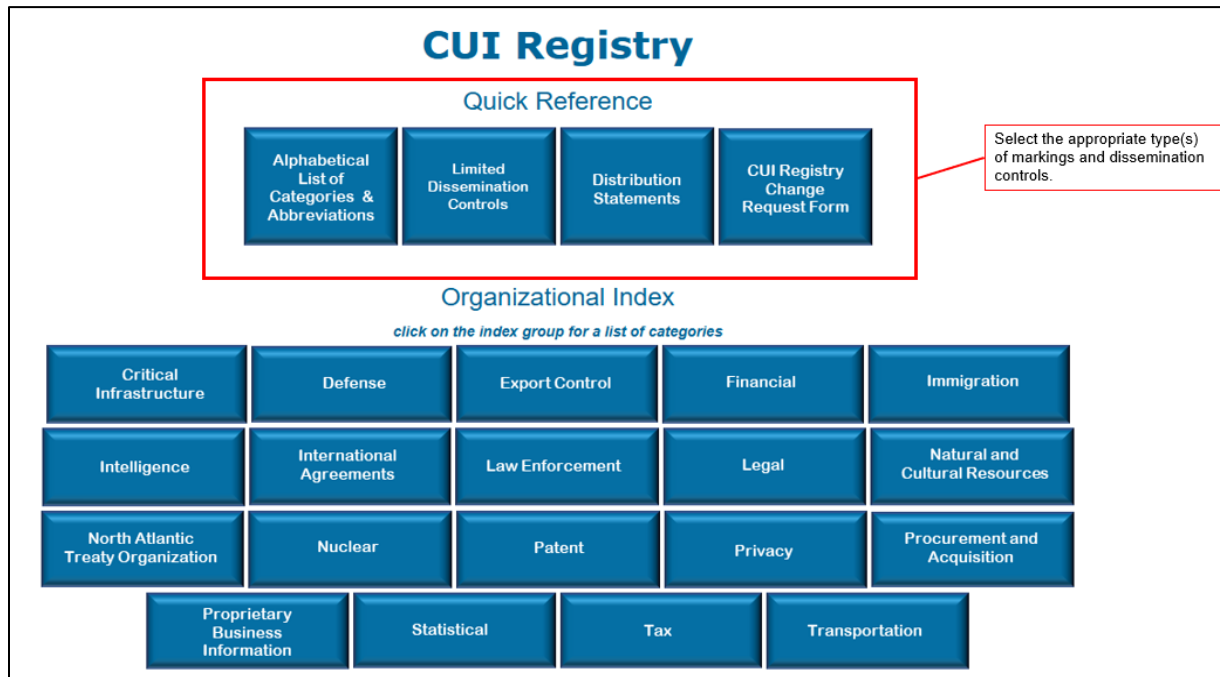


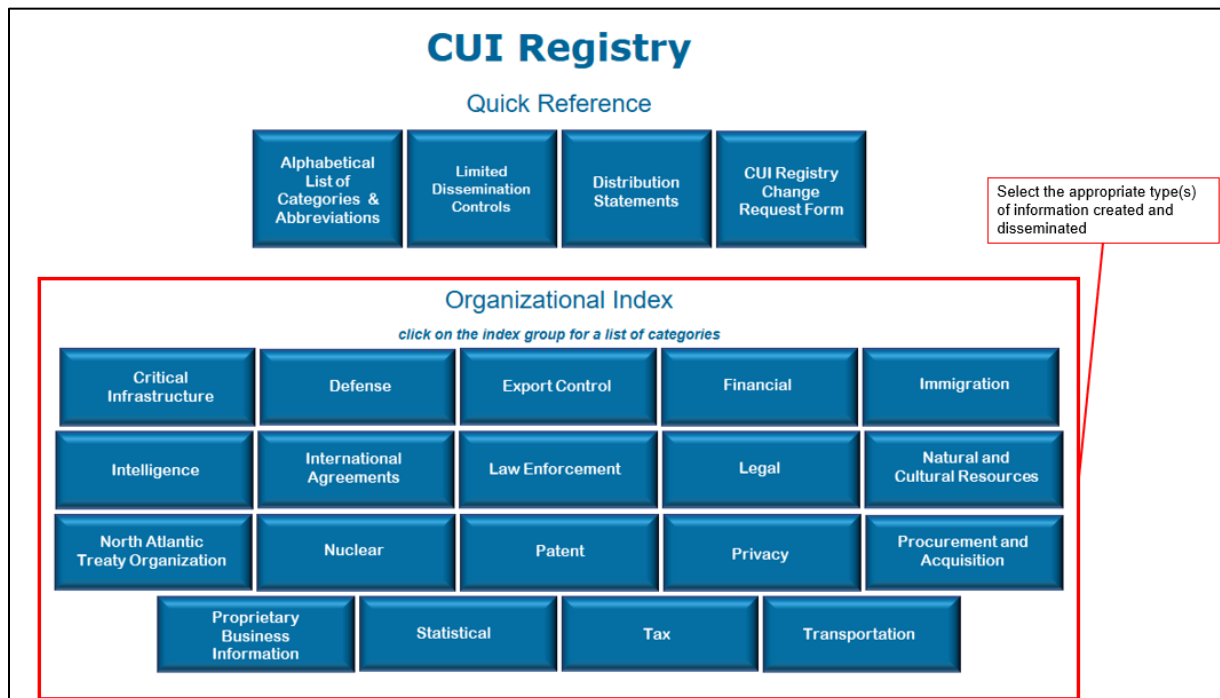
Figure 1. CUI Determination Flowchart

## ATTACHMENT C

### CONTROLLED UNCLASSIFIED INFORMATION REGISTRY



**Figure 2.** Screenshot from CUI Registry Quick Reference (See reference g.)



**Figure 3.** Screenshot from CUI Registry Quick Reference (See reference g.)

## ATTACHMENT D

## CONTROLLED UNCLASSIFIED INFORMATION DISSEMINATION CONTROLS

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

- 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.

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 (SFDR) to make further sharing decisions for unclassified 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. <a href="#">See list of approved country codes.</a>
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.

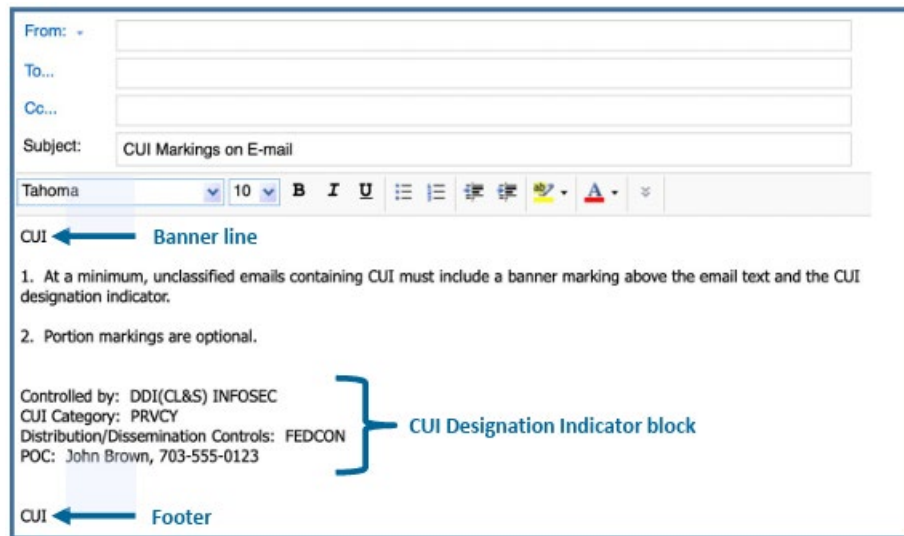
\* DL ONLY is used when you have a specific organization or list of individuals authorized to receive the document and none of the other LDCs apply. The list must be on or attached to the document, or a link to the list annotated on the document.

**Figure 4.** Screenshot from Cleared CUI Dissemination Control Training Aid

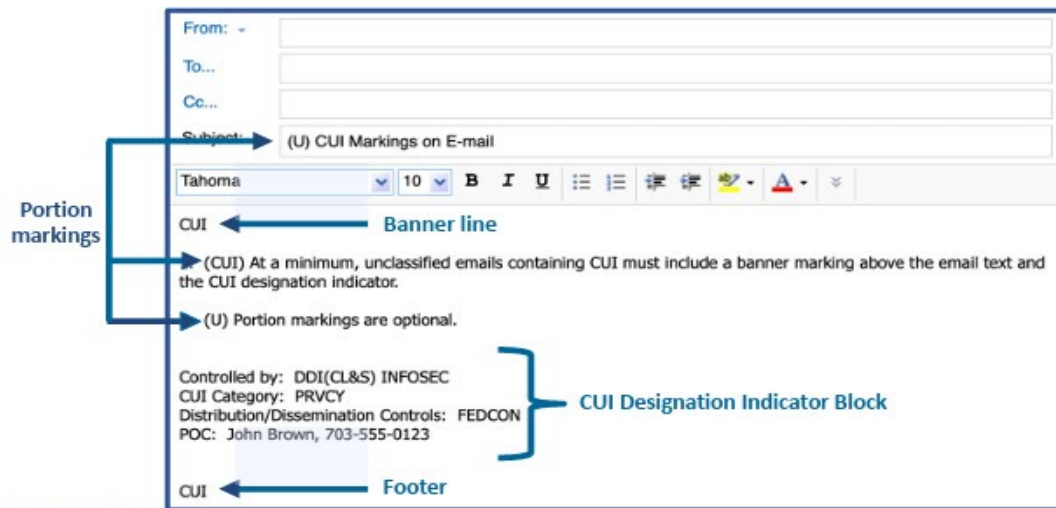


## ATTACHMENT E

### EMAIL CONTROLLED UNCLASSIFIED INFORMATION MARKING GUIDE



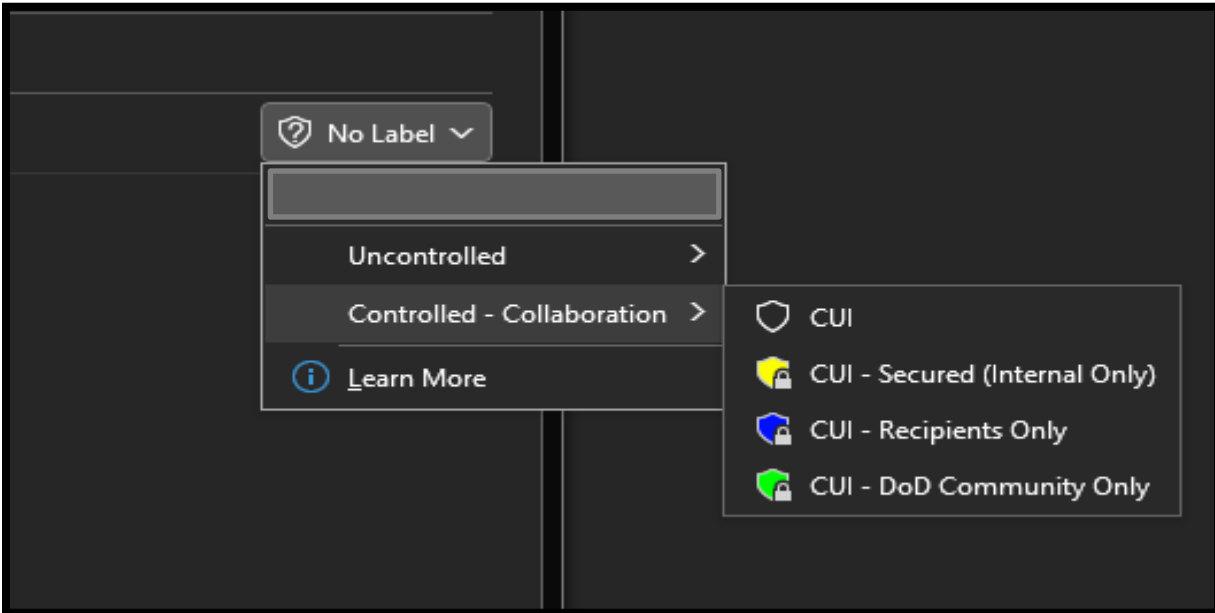
**Figure 5.** Email CUI Marking Example



**Figure 6.** Email CUI Marking Example with Correct Portion Markings

## ATTACHMENT F

### MICROSOFT OFFICE 365 OUTLOOK CONTROLLED UNCLASSIFIED INFORMATION LABELING TOOL

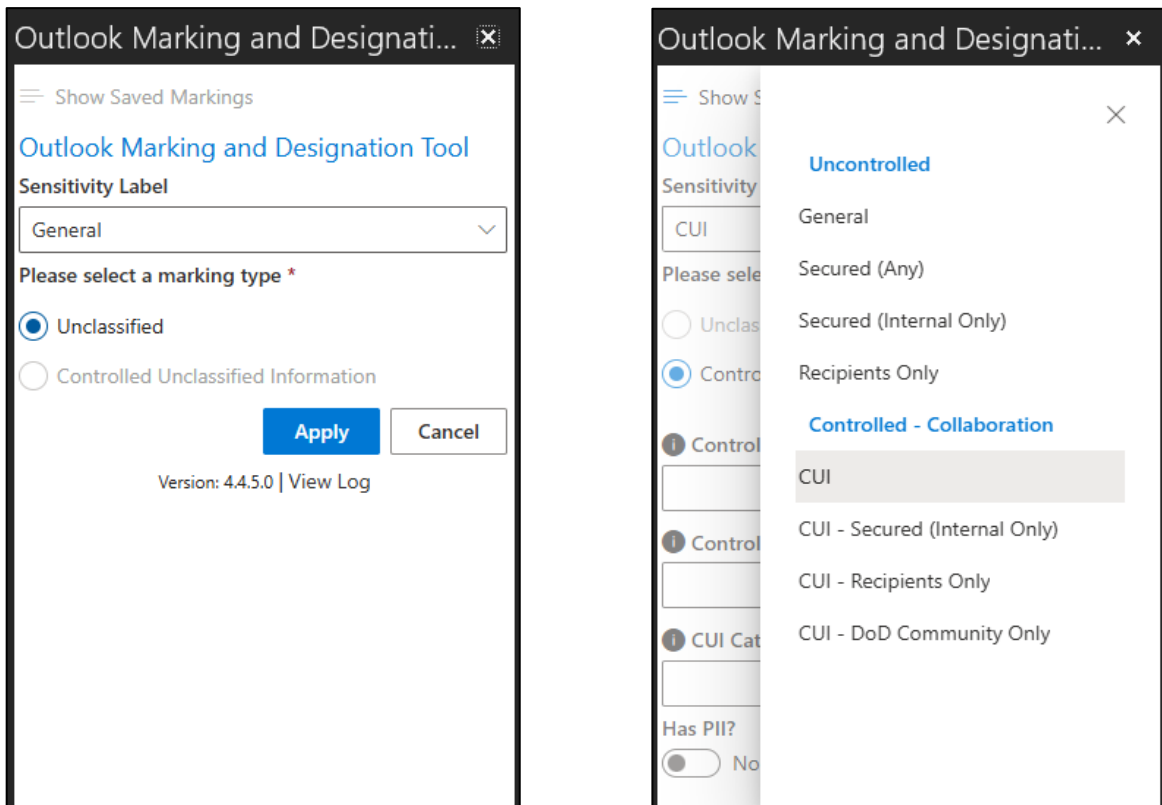
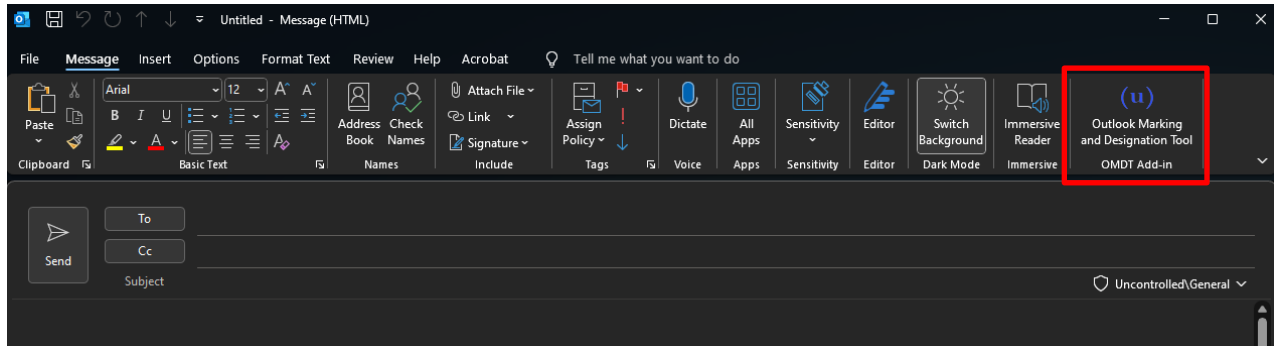


**Figure 7.** Screenshot from Microsoft Office 365 Outlook Classic CUI Encryption Tool

1. CUI. Access and Restrictions will apply for sharing with external commercial accounts. Email must be manually encrypted and follow CUI email marking requirements.
2. CUI Secured (Internal Only). Access and Distribution are restricted to internal (A365) users only. For tool auto-encrypted email, follow CUI email marking requirements.
3. CUI Recipients Only. Custom Access and Distribution control as defined by content or the email originator, including ability to restrict recipients' ability to forward, print, or copy content. For tool auto-encrypted email, follow CUI email marking requirements.
4. CUI DoD Community Only. Access and Distribution are restricted to users within the DoD Community (Microsoft Office 365 DoD users). For tool auto-encrypted email, follow CUI email marking requirements.

## ATTACHMENT G

### MICROSOFT OFFICE 365 OUTLOOK MARKING AND DESIGNATION TOOL



**Figure 8.** Screenshots from Microsoft Office 365 Outlook Classic Marking and Designation Tool

1. CUI. Access and Restrictions will apply for sharing with external commercial accounts. Email must be manually encrypted and follow CUI email marking requirements.
2. CUI -- Secured (Internal Only). Access and Distribution are restricted to internal (A365) users only. For tool auto-encrypted email, follow CUI email marking requirements.

3. CUI -- Recipients Only. Custom Access and Distribution control is defined by content or email originator, including ability to restrict recipients' ability to forward, print, or copy content. For tool auto-encrypted email, follow CUI email marking requirements.
4. CUI -- DoD Community Only. Access and Distribution restricted to users within the DoD Community (Microsoft Office 365 DoD users). For tool auto-encrypted email, follow CUI email marking requirements.

## ATTACHMENT H

### DOCUMENT CONTROLLED UNCLASSIFIED INFORMATION MARKING GUIDE

**CUI Markings (text documents)**

Step 1: apply portion marks (title, subject, paragraphs, sub-paragraphs, bullet points, sub-bullet points, graphs, etc.). Do not portion the signature block or CUI designation indicator block.

**NOTE: Portion marking is optional, but strongly recommended, in unclassified documents.**

Step 2: place "CUI" at the top and bottom of each page.

Step 3: place the CUI designation indicator block at the bottom of the first page or cover page.

The screenshot shows a memorandum from the Office of the Under Secretary of Defense, Intelligence and Security. The document is titled 'MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP (SEE DISTRIBUTION) DEFENSE AGENCY AND DOD FIELD ACTIVITY DIRECTORS'. The subject line is '(U) Fiscal Year 2020 Information Security Oversight Office Annual Reporting Requirements'. The body text discusses the request from the Information Security Oversight Office (ISOO) regarding the impact of the COVID-19 pandemic. The signature block is for Bill Smith, Deputy Director. At the bottom, there is a control block with the following text: 'Controlled by: DDI/CL&S', 'CUI Category: BUDG', 'Limited Dissemination Control: FEDCON', and 'POC: Stan Jones, 703-555-9512'. The document is marked with 'CUI' at the top and bottom. Training aid annotations include: 'Step 1' pointing to the subject line and the first paragraph; 'Step 2' pointing to the 'CUI' markings at the top and bottom; and 'Step 3' pointing to the control block at the bottom.

**Figure 9.** Screenshot from Cleared CUI Document Marking Training Aid

## ATTACHMENT I

### POWERPOINT CONTROLLED UNCLASSIFIED INFORMATION MARKING GUIDE

**CUI Markings (slide presentations)**

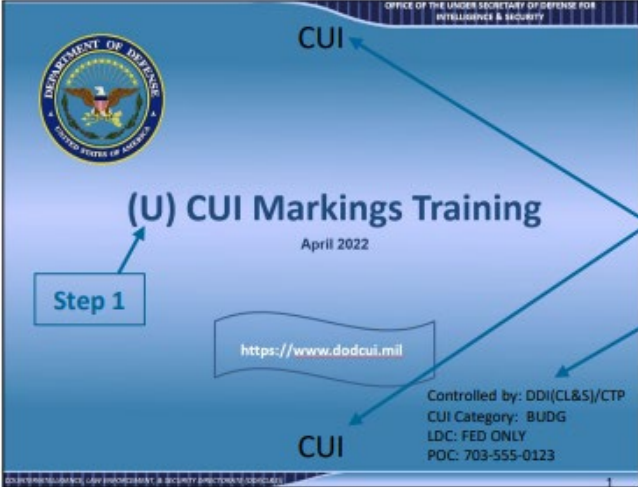
Step 1: apply portion marks (title, subject, paragraphs, sub-paragraphs, bullet points, sub-bullet points, graphs, etc.). Do not portion mark the signature block or CUI designation indicator block.

**NOTE: Portion marking is optional, but strongly recommended, in unclassified documents.**

Step 2: place "CUI" at the top and bottom of each page.

Step 3: place the CUI designation indicator block at the bottom of the first page, or cover.

#### Cover Slide



The cover slide features the Department of Defense seal, the title "(U) CUI Markings Training", the date "April 2022", the URL "https://www.dodcui.mil", and a control block at the bottom right: "Controlled by: DDI(CL&S)/CTP", "CUI Category: BUDG", "LDC: FED ONLY", and "POC: 703-555-0123". Annotations show "CUI" at the top and bottom, and the control block at the bottom right.

**Step 1:** Points to the title "(U) CUI Markings Training".

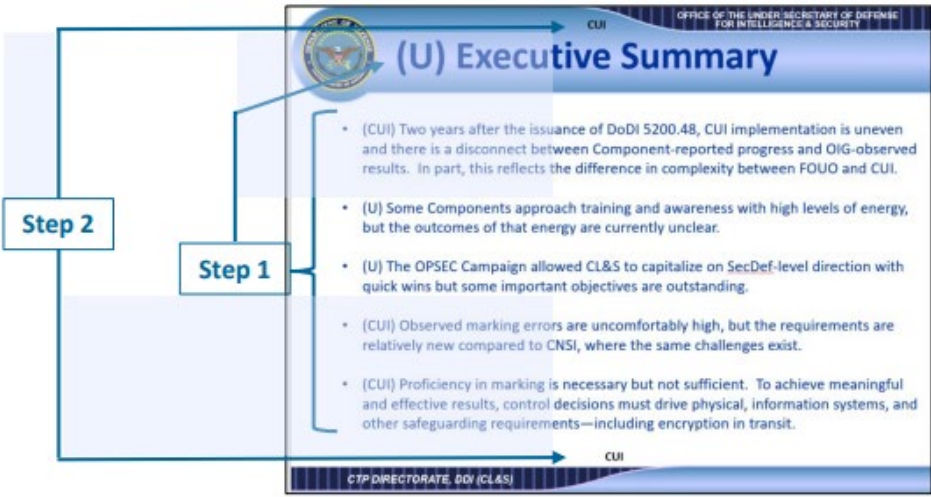
**Step 2:** Points to the "CUI" text at the top of the slide.

**Step 3:** Points to the CUI designation indicator block at the bottom right.

The markings in the header and footer on the cover slide reflect the overall marking for the presentation, not the cover slide itself.

The markings in the header and footer on subsequent slides reflect either the overall marking, or the marking for each individual slide. Be consistent in how you mark interior slides. Either mark all interior slides with the overall marking or mark all interior slides individually.

#### Interior Slide



The interior slide features the Department of Defense seal, the title "(U) Executive Summary", and a list of bullet points. Annotations show "CUI" at the top and bottom, and the control block at the bottom right: "CTP DIRECTORATE, DDI (CL&S)".

**Step 1:** Points to the title "(U) Executive Summary".

**Step 2:** Points to the "CUI" text at the top of the slide.

**Back to TOC** link is visible in the bottom left corner.

Figure 10. Screenshot from Cleared CUI Training Aid

## ATTACHMENT J

### REFERENCES

#### PART I. REQUIRED

- a. Department of Defense (DoD) Intelligence and Security CUI Registry, <https://www.dodcui.mil/CUI-Registry-New/>, accessed 05 August 2025
- b. DoD Instruction 5200.48, 06 March 2020, "Controlled Unclassified Information"
- c. DoD Instruction 8500.01, 07 October 2019, "Cybersecurity"
- d. DoD Manual 5200.01, Volumes 1, 28 July 2020, "DoD Information Security Program: Overview, Classification, and Declassification"
- e. DoD Manual 5200.01, Volume 2, 28 July 2020, "DoD Information Security Program: Marking of Information"
- f. DoD Manual 5200.01, Volume 3, 28 July 2020, "DoD Information Security Program: Protection of Classified Information"
- g. DoD Quick Reference Guide, December 2024, "CUI Quick Reference Guide," <[https://www.dodcui.mil/Portals/109/Documents/Desktop%20Aid%20Docs/Cleared%20CUI%20Quick%20Reference%20Guide%20October%202024.pdf?ver=Bsk1IElIkzFNnSO\\_jjqUmA%3d%3d](https://www.dodcui.mil/Portals/109/Documents/Desktop%20Aid%20Docs/Cleared%20CUI%20Quick%20Reference%20Guide%20October%202024.pdf?ver=Bsk1IElIkzFNnSO_jjqUmA%3d%3d)>, accessed 05 August 2025

#### PART II. RELATED

- h. The White House, Executive order 13526, 29 December 2009, "Classified National Security Information," <<https://www.archives.gov/isoo/policy-documents/cnsi-eo.html>>, accessed 05 August 2025
- i. The White House, Executive order 13556, 04 November 2010, "Controlled Unclassified Information," <<https://obamawhitehouse.archives.gov/the-press-office/2010/11/04/executive-order-13556-controlled-unclassified-information>>, accessed 05 August 2025
- j. Chief of the National Guard Bureau Instruction 5000.01C, 24 January 2020, "Chief of the National Guard Bureau Issuances Program"
- k. Center for Development of Security Excellence, Defense Counterintelligence and Security Agency Security Awareness Hub security training website, <<https://securityawareness.usalearning.gov/>>, accessed 05 August 2025

I. 32 Code of Federal Regulations, "National Archives and Records Administration,"  
Part 2001, 28 June 2010, "Classified National Security Information"



## GLOSSARY

### PART I. ACRONYMS

CDSE	Center for Development of Security Excellence
CNGB	Chief of the National Guard Bureau
CNGB DTM	Chief of the National Guard Bureau Directive-Type Memorandum
CUI	Controlled Unclassified Information
DoD	Department of Defense
INFOSEC	Information Security
NGB	National Guard Bureau
NGB-J2	National Guard Bureau Joint Intelligence Directorate
NGB-J24	Counterintelligence and Security Division

### PART II. DEFINITIONS

CUI -- (Controlled Unclassified Information) is 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 safeguarding or dissemination controls.

CUI Custodian -- A Controlled Unclassified Information custodian is anyone who handles, creates, receives, communicates or transmits Controlled Unclassified Information. Also referred to as the information owner due to possession of such information.

CUI Registry -- Controlled Unclassified Information Registry is the online repository for all information, guidance, policy, and requirements on handling. Among other information, the Controlled Unclassified Information Registry identifies all approved Controlled Unclassified Information categories and subcategories, provides general descriptions for each, identifies the basis for controls, establishes markings, and includes guidance on handling procedures.