DoD Instruction 5200.48

Controlled Unclassified Information (CUI)

Originating Component:	Office of the Under Secretary of Defense for Intelligence and Security
Effective:	March 6, 2020
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Cancels:	DoD Manual 5200.01, Volume 4, "DoD Information Security Program: Controlled Unclassified Information," February 24, 2012, as amended
Approved by:	Joseph D. Kernan, Under Secretary of Defense for Intelligence and Security (USD(I&S))

Purpose: In accordance with the authority in DoD Directive (DoDD) 5143.01 and the December 22, 2010 Deputy Secretary of Defense Memorandum, this issuance:

- Establishes policy, assigns responsibilities, and prescribes procedures for CUI throughout the DoD in accordance with Executive Order (E.O.) 13556; Part 2002 of Title 32, Code of Federal Regulations (CFR); and Defense Federal Acquisition Regulation Supplement (DFARS) Sections 252.204-7008 and 252.204-7012.
- Establishes the official DoD CUI Registry.

TABLE OF CONTENTS

TABLES

FIGURES

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

This issuance applies to:

a. Office of the Secretary of Defense (OSD), the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense (OIG DoD), the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this issuance as the "DoD Components").

b. Arrangements, agreements, contracts, and other transaction authority actions requiring access to CUI according to terms and conditions of such documents, as defined in Clause 2.101 of the Federal Acquisition Regulation and Section 2002.4 of Title 32, CFR, including, but not limited to, grants, licenses, certificates, memoranda of agreement/arrangement or understanding, and information-sharing agreements or arrangements.

1.2. POLICY.

It is DoD policy that:

a. As part of the phased DoD CUI Program implementation process endorsed by the CUI Executive Agent (EA) pursuant to Information Security Oversight Office (ISOO) Memorandum dated August 21, 2019, the designation, handling, and decontrolling of CUI (including CUI identification, sharing, marking, safeguarding, storage, dissemination, destruction, and records management) will be conducted in accordance with this issuance and Sections 252.204-7008 and 252.204-7012 of the DFARS when applied by a contract to non-DoD systems.

b. All DoD CUI must be controlled until authorized for public release in accordance with DoD Instructions (DoDIs) 5230.09, 5230.29, and 5400.04, or DoD Manual (DoDM) 5400.07. Official DoD information that is not classified or controlled as CUI will also be reviewed prior to public release in accordance with DoDIs 5230.09 or5230.29.

c. Information will not be designated CUI in order to:

(1) Conceal violations of law, inefficiency, or administrative error.

(2) Prevent embarrassment to a person, organization, or agency.

(3) Prevent open competition.

(4) Control information not requiring protection under a law, regulation, or government-wide policy, unless approved by the CUI EA at the National Archives and Records Administration (NARA), through the Under Secretary of Defense for Intelligence and Security (USD(I&S)).

d. In accordance with the DoD phased CUI Program implementation, all documents containing CUI must carry CUI markings in accordance with this issuance.

e. Although DoD Components are not required to use the terms "Basic" or "Specified" to characterize CUI at this time, DoD Components will apply:

(1) At least the minimum safeguards required to protect CUI.

(2) Terms and specific marking requirements will be promulgated by the USD(I&S) in future guidance.

f. Nothing in this issuance alters or supersedes the existing authorities of the Director of National Intelligence (DNI) regarding CUI.

g. Nothing in this issuance will infringe on the OIG DoD's statutory independence and authority, as articulated in the Inspector General Act of 1978 in the Title 5, United States Code (U.S.C.) Appendix. In the event of any conflict between this instruction and the OIG DoD's statutory independence and authority, the Inspector General Act of 1978 in the Title 5, U.S.C. Appendix takes precedence.

SECTION 2: RESPONSIBILITIES

2.1. USD(I&S)

The USD(I&S):

a. As the DoD Senior Agency Official for Security, establishes policy and oversees the DoD Information Security Program.

b. In coordination with the requesting DoD Component, submits changes to CUI categories on behalf of DoD Components to the CUI EA at NARA.

c. Provides reports to the CUI EA on the DoD CUI Program status, as described in Paragraph 3.6.c., in accordance with Part 2002 of Title 32, CFR.

d. Establishes protocol for resolving disputes about implementing or interpreting E.O. 13556, Part 2002 of Title 32, CFR, the CUI Registry, and this issuance, within and between the DoD Components.

e. Coordinates with the Department of Defense Chief Information Officer (DoD CIO) on CUI waiver requests for DoD information systems (IS) and networks.

f. Coordinates with the CUI EA on DoD Component CUI waiver requests.

2.2. DIRECTOR FOR DEFENSE INTELLIGENCE (COUNTERINTELLIGENCE, LAW ENFORCEMENT, AND SECURITY (DDI(CL&S)).

The DDI(CL&S):

a. Oversees and manages the DoD CUI Program.

b. Reviews and signs all reports and other correspondence related to the DoD CUI Program.

c. Coordinates with the Secretaries of the Military Departments, Under Secretary of Defense for Research and Engineering (USD(R&E)), Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)), and the DoD Component heads to:

(1) Recommend changes to national CUI policy relating to identifying, safeguarding, disseminating, marking, storing, transmitting, reviewing, transporting, re-using, decontrolling, and destroying CUI, and responding to unauthorized disclosure (UD) of CUI.

(2) Review and provide guidance on DoD Component implementation policy and CUI-related matters.

d. Assists the USD(I&S) with overseeing the CUI policy and program execution via the Defense Security Enterprise Executive Committee in accordance with DoDD 5200.43.

e. In coordination with the DoD CIO, USD(A&S), and USD(R&E), provides guidance on implementing uniform standards to display TOP SECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED for CNSI and CUI controls and banners for DoD systems and networks.

2.3. DIRECTOR, DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY (DSCA).

Under the authority, direction, and control of the USD(I&S) and in addition to the responsibilities in Paragraph 2.10., the Director, DCSA:

a. Administers the DoD CUI Program for contractually established CUI requirements for contractors in classified contracts in accordance with the May 17, 2018 Under Secretary of Defense for Intelligence Memorandum.

b. Assesses contractor compliance with contractually established CUI system requirements in DoD classified contracts associated with the National Industrial Security Program (NISP) in accordance with Part 2003 of Title 32, CFR and National Institute of Standards and Technology Special Publication (NIST SP) 800-171 guidelines.

c. Establishes and maintains a process to notify the DoD CIO, USD(R&E), and USD(A&S) of threats related to CUI for further dissemination to DoD Components and contractors in accordance with the Section 252.204-7012 of the DFARS.

d. Provides, in coordination with the USD(I&S), security education, training, and awareness on the required topics identified in Section 2002.30 of Title 32, CFR, including protection and management of CUI, to DoD personnel and contractors through the Center for Development of Security Excellence (CDSE).

e. Provides security assistance and guidance to the DoD Components on the protection of CUI when DoD Components establish CUI requirements in DoD classified contracts for NISP contractors falling under DCSA security oversight.

f. Serves as the DoD-lead to report UDs of CUI, except for the reporting of cyber incidents in accordance with Section 252.204-7012 of the DFARS, associated with contractually established CUI system requirements in DoD classified contracts for NISP contractors falling under DCSA security oversight.

g. Coordinates with the DoD CIO to implement uniform security requirements when the IS or network security controls for unclassified and classified information are included in DoD classified contracts for NISP contractors falling under DCSA security oversight.

h. Consolidates DoD Component input on the oversight of CUI protection requirements in DoD classified contracts for NISP contractors under DCSA security oversight, as required by Information Security Oversight Office (ISOO) Notice 2016-01.

2.4. CHIEF MANAGEMENT OFFICER OF THE DEPARTMENT OF DEFENSE (CMO).

In addition to the responsibilities in Paragraph 2.10., the CMO:

a. Serves as the subject matter expert on CUI containing personally identifiable information and its release in accordance with Subsection 552 of Chapter 5 of Title 5, United States Code (U.S.C.), also known as and referred to in this issuance as the "Freedom of Information Act (FOIA)," implemented through DoDD 5400.07 and DoDI 5400.11, and Subsection 552a of Chapter 5 of Title 5, U.S.C., also known and referred to in the issuance as the "Privacy Act of 1974."

b. Supports OSD with information security matters, as appropriate.

2.5. PFPA.

Under the authority, direction, and control of the CMO, through the Director for Administration and Organizational Policy, and in addition to the responsibilities in Paragraph 2.10., the Director, PFPA:

a. Provides information security administrative support to OSD.

b. Provides information on OSD CUI Program status and other formally requested assistance to the USD(I&S) to support the CUI Program.

c. Conducts CUI staff assistance visits to OSD in the National Capital Region.

2.6. UNDER SECRETARY OF DEFENSE FOR POLICY.

In addition to the responsibilities in Paragraph 2.10., the Under Secretary of Defense for Policy:

a. Establishes policy and procedures for disclosing DoD CUI to foreign governments, the North Atlantic Treaty Organization, and international organizations based on formally signed agreements and arrangements between the parties.

b. Requires CUI to be identified in international agreements, arrangements, and contracts having licensing export controls for foreign partners.

2.7. USD(A&S).

In addition to the responsibilities in Paragraph 2.10., pursuant to Section 133b of Title 10, U.S.C., and in coordination with the USD(I&S), DoD CIO, and USD(R&E), the USD(A&S):

a. Maintains, in accordance with Section 252.204-7012 of the DFARS, DoD acquisition contracting processes, policies, and procedures for safeguarding DoD CUI in DoD procurement arrangements, agreements, and contracts, including other transaction authority actions.

b. Supports the development and implementation of a Federal Acquisition Regulation clause applying CUI requirements to defense contractors.

2.8. USD(R&E).

In addition to the responsibilities in Paragraph 2.10., pursuant to Section 133a of Title 10, U.S.C., and in coordination with USD(I&S), the USD(R&E):

a. Establishes DoD CUI processes, policies, and procedures for grants and cooperative research and development arrangements, agreements, and contracts involving controlled technical information (CTI).

b. Establishes a standard process to identify CTI; guidelines for sharing, marking, safeguarding, storing, disseminating, decontrolling, and destroying CTI; and CTI records management requirements contained in contracts, as appropriate.

c. Oversees and ensures DoD CUI guidelines and requirements for sharing, marking, safeguarding, storage, dissemination, decontrol, destruction, and records management of all research, development, test, and evaluation information are properly executed for all DoD owned records.

d. In coordination with the USD(A&S), ensures:

(1) Contracts, arrangements, and agreements for research, development, testing, and evaluation identify CUI at the time of award.

(2) USD(R&E) international agreements, arrangements, and contracts with foreign partners identify CUI within the documents.

(3) DoD Components concluding international agreements, arrangements, and contracts with foreign partners include U.S. Government-approved text on CUI.

2.9. DOD CIO.

In addition to the responsibilities in Paragraph 2.10., the DoD CIO:

a. Oversees CUI metadata tagging standards, consistent with federal data tagging approaches in accordance with the National Strategy for Information Sharing and Safeguarding, to implement the marking requirements in Paragraph 3.4.c. and in accordance with DoDI 8320.07.

b. Integrates CUI metadata tagging standards into DoD information technology content management tools to support discovery, access, auditing, safeguarding, and records management decisions regarding CUI (including monitoring CUI data for visibility, accessibility, trust, interoperability, and comprehension).

c. Provides policy and standards recommendations to the USD(I&S) on updates for the sharing, marking, safeguarding, storage, dissemination, decontrol, destruction, and records

management of DoD CUI residing on both DoD and non-DoD IS in accordance with DoDI 8582.01.

d. Oversees Defense Industrial Base Cybersecurity Activities, using the DoD Cyber Crime Center as the single DoD focal point for receiving and disseminating all cyber incident reports impacting unclassified networks of defense contractors.

e. Coordinates with the USD(I&S), USD(A&S), USD(R&E), and DoD Component heads to develop uniform security requirements for industry partners' IS and network security controls adequate for the type of CUI identified in the contract in accordance with Part 2002 of Title 32, CFR, Section 252.204-7012 of the DFARS, and NIST SP 800-171.

f. Coordinates with the Director, DCSA to implement uniform security requirements when IS or network security controls for unclassified and classified information are included in DoD classified contracts of NISP contractors falling under DCSA security oversight.

g. Coordinates with the USD(I&S) to:

(1) Implement information security policy standards for markings to display, CUI for DoD classified and unclassified systems and networks.

(2) Integrate training on safeguarding and handling CUI into updates to initial and annual cybersecurity awareness training.

h. Notifies the CUI EA in coordination with the USD(I&S) of CUI waivers impacting IS or networks in accordance with Title 32 of the CFR.

i. Oversees and ensures DoD Component- and National Archives-approved disposition authorities for CUI are implemented for DoD records and information.

j. Oversees and ensures the Director, DoD Cyber Crime Center:

(1) Manages and updates, as necessary and in coordination with DoD CIO, the policies in Section 236.4 of Title 32, CFR and Section 252.204-7012 of the DFARS.

(2) Maintains the website at https://dibnet.dod.mil to receive contractor mandatory incident reports in accordance with Paragraph 3.9.d(1).

2.10. OSD AND DOD COMPONENT HEADS.

OSD and DoD Component heads:

a. Identify, program, and commit the necessary resources to implement CUI Program requirements as part of their overall information security programs.

b. Designate in writing (with copy to the USD(I&S)):

(1) A DoD Component senior agency official (CSAO) at the Senior Executive Service level or equivalent to implement their CUI Program and perform the duties in Paragraph 3.5.

(2) A DoD Component program manager (CPM) to manage their CUI Program.

c. Ensure their subordinate organizations comply with DoD CUI Program requirements.

d. Ensure their personnel receive initial and annual refresher CUI education and training, and maintain documentation of this training for audit purposes.

e. Report DoD Component training completion data to the USD(I&S) annually or as directed.

f. Provide an annual report to the USD(I&S) on CUI implementation status in accordance with Title 32, CFR, Part 2002.

g. Determine if any CUI documents or materials constitute permanently valuable records of the government, which require maintenance and disposal in accordance with DoDI 5015.02.

h. As the requiring activity, oversee CUI requirements for contractor implementation in partnership with the Defense Contract Management Agency, based on Defense Contract Management Agency responsibilities, or DCSA for cleared contractors in accordance with the NISP, as appropriate.

i. Ensure DoD Component- and National Archives-approved disposition authorities are implemented for DoD records and information regardless of classification.

j. Manage their CUI programs in accordance with guidelines prescribed in this DoD issuance.

2.11. SECRETARIES OF THE MILITARY DEPARTMENTS.

In addition to the responsibilities in Paragraph 2.10., the Secretaries of the Military Departments oversee the implementation of their CUI programs.

2.12. CHAIRMAN OF THE JOINT CHIEFS OF STAFF.

In addition to the responsibilities in Paragraph 2.10., the Chairman of the Joint Chiefs of Staff oversees the implementation of the CUI programs in the Joint Staff organizations and Combatant Commands.

SECTION 3: PROGRAMMATICS

3.1. BACKGROUND.

The CUI EA at NARA, through the Information Security and Oversight Office (ISOO), published and released Part 2002 of Title 32, CFR, which provides implementing requirements for E.O. 13556.

a. Part 2002 of Title 32, CFR established a CUI EA office under NARA's ISOO for implementing and overseeing the CUI Program.

b. Designed as a response to the information sharing challenges from inconsistent definitions and marking requirements applied to CUI, Part 2002 of Title 32 CFR standardized the definition of CUI and codified the identification, sharing, safeguarding, marking, storage, distribution, transmission, decontrol, destruction, training, monitoring, and reporting requirements across the Executive branch of government.

c. In accordance with Part 2002 of Title 32, CFR, CUI requires safeguarding or dissemination controls identified in a law, regulation, or government-wide policy for information that does not meet the requirements for classification in accordance with E.O. 13526.

d. Unlike classified information, an individual or organization generally does not need to demonstrate a need-to-know to access CUI, unless required by a law, regulation, or government-wide policy, but must have a lawful governmental purpose for such access. One example of a requirement for need-to-know established by law, regulation, or government-wide policy is Section 223.6 of Title 32, CFR, which requires a person to have a need-to-know to be granted access to DoD Unclassified Nuclear Information (UCNI).

3.2. LEGACY INFORMATION REQUIREMENTS.

This legacy information guidance applies to information contained across DoD in, among other documents, security classification guides (SCGs), various policies, and other legacy materials falling under the Science and Technology Information Program (DoDI 3200.12), in either electronic or hardcopy format. The CUI Program does not require the redacting or re-marking of documents bearing legacy markings. However, any new document created with information derived from legacy material must be marked as CUI if the information qualifies as CUI.

a. DoD legacy material will not be required to be re-marked or redacted while it remains under DoD control or is accessed online and downloaded for use within the DoD. However, any such document or new derivative document must be marked as CUI if the information qualifies as CUI and the document is being shared outside DoD. DoD legacy marked information stored on a DoD access-controlled website or database does not need to be remarked as CUI, even if other agencies and contractors are granted access to such websites or databases.

b. DoD legacy information does not automatically become CUI. It must be reviewed by the owner of the information to determine if it meets the CUI requirements. If it is determined the

specific legacy information meets the CUI requirements, it will be marked in accordance with this issuance and corresponding manual.

c. For federal systems, IS storing information identified as CUI must meet the minimum network security standard in Part 2002 of Title 32, CFR. For nonfederal systems, IS must meet the standards in the NIST SP 800-171, when established by contract.

d. When DoD legacy information is incorporated into, or cited in, another document or material, it must be reviewed for CUI and marked in accordance with this issuance.

3.3. HANDLING REQUIREMENTS.

The DoD CUI Information Security Program will promote, to the maximum extent possible, information sharing, facilitate informed resource use, and simplify its management and implementation while maintaining required safeguarding and handling measures.

a. In accordance with DoDI 5230.09 and the August 14, 2014 Deputy Secretary of Defense Memorandum:

(1) The DoD originator or authorized CUI holder must ensure a prepublication and security policy review is conducted, pursuant to the standard DoD Component process, before CUI is approved for public release, which includes publication to a publicly accessible website.

(2) Decontrolling and releasing CUI records will be executed by the originator of the information, the original classification authority (OCA) if identified in a security classification guide, or designated offices for decontrolling CUI pursuant to the procedures for the review and release of information under the FOIA in accordance with the November 19, 2018 ISOO Notice. There are no specific timelines to decontrol CUI unless specifically required in a law, regulation, or government-wide policy. Decontrol will occur when the CUI no longer requires safeguarding and will follow DoD records management procedures.

b. OCAs will determine if aggregated CUI under their control should be classified in accordance with Volume 1 of DoDM 5200.01 and will confirm the relevant SCGs address the compilation.

c. DoD information systems processing, storing, or transmitting CUI will be categorized at the "moderate" confidentiality impact level and follow the guidance in DoDIs 8500.01 and 8510.01. Non-DoD information systems processing, storing, or transmitting CUI will provide adequate security, and the appropriate requirements must be incorporated into all contracts, grants, and other legal agreements with non-DoD entities in accordance with DoDI 8582.01. See Section 5 of this issuance for more information on CUI and its application to industry.

d. The DoD CUI Registry provides an official list of the Indexes and Categories used to identify the various types of DoD CUI. The DoD CUI Registry mirrors the National CUI Registry, but provides additional information on the relationships to DoD by aligning each Index and Category to DoD issuances.

(1) The official DoD CUI Registry of categories can be accessed on Intelink at https://intelshare.intelink.gov/sites/ousdi/hcis/sec/icdirect/information/CUI/Forms/AllItems.aspx.

(2) The site will be updated as changes to the DoD CUI Registry are made based on official notification from the CUI EA through the CUI Registry Working Group; changes to law, regulation, or government-wide policy; or notification that the information no longer meets the requirements for CUI.

3.4. MARKING REQUIREMENTS.

This paragraph covers the essential marking requirements for initial phased implementation of the DoD CUI Program.

a. At minimum, CUI markings for unclassified DoD documents will include the acronym "CUI" in the banner and footer of the document.

b. If portion markings are selected, then all document subjects and titles, as well as individual sections, parts, paragraphs, or similar portions of a CUI document known to contain CUI, will be portion marked with "(CUI)." Use of the unclassified marking "(U)" as a portion marking for unclassified information within CUI documents or materials is required.

(1) There is no requirement to add the "U," signifying unclassified, to the banner and footer as was required with the old FOUO marking (i.e., U//FOUO).

(2) Banners, footers, and portion marking will only be marked "Unclassified" or "(U)" for unclassified information in accordance with the June 4, 2019 ISOO letter. If the document also contains CUI, it will be marked in accordance with Paragraph 3.4.a. and additional forthcoming guidance.

c. CUI markings in classified documents will appear in paragraphs or subparagraphs known to contain **only** CUI and must be portion marked with "(CUI)." "CUI" will **not** appear in the banner or footer.

(1) There will be an acknowledgement added to the warning box on the first page of multi-page documents to alert readers to the presence of CUI in a classified DoD document, as shown in Figure 1.

Figure 1. CUI Warning Box for Classified Material

This content is classified at the [insert highest classification level of the source data] level and may contain elements of controlled unclassified information (CUI), unclassified, or information classified at a lower level than the overall classification displayed. This content shall not be used as a source of derivative classification; refer instead to [cite specific reference, where possible, or state "the applicable classification guide(s)"]. It must be reviewed for both Classified National Security Information (CNSI) and CUI in accordance with DoDI 5230.09 prior to public release. [Add a point of contact when needed.]

(2) Volume 2 of DoDM 5200.01 requires DoD intelligence producers to follow DNI formats for intelligence production under the authority of the DNI. When DoD CUI is incorporated into a Digital Access Policy under the authority of the DNI, the information and the document will follow the Digital Access Policy standards established by the DNI.

d. The dissemination marking "not releasable to foreign nationals (NOFORN or NF)" is an intelligence control marking used to identify intelligence information an originator has determined meets the criteria of Intelligence Community Directive 710 and Intelligence Community Policy Guidance 403.1, which provides guidance for further dissemination control markings. It must be applied to controlled unclassified intelligence information that is properly characterized as CUI with appropriate CUI markings. CUI identified with this marking will not be provided, in any form, to foreign governments (including coalition partners), international organizations, foreign nationals, or other non-U.S. persons without the originator's approval in accordance with E.O.s 13526 and 13556. If originator approval is required for further dissemination, the originator will mark the requirement on the information in accordance with Section 4.1(i)(1) of E.O. 13526.

(1) The application of the control marking "not releasable to foreign nationals" (NOFORN or NF) will only be applied, when warranted, to unclassified intelligence information properly categorized as CUI and reviewed by a Foreign Disclosure Officer to ensure there are no international agreements in place to prohibit its use and prohibiting sharing.

(2) The control marking NOFORN or NF will be applied to Naval Nuclear Propulsion Information (NNPI), Unclassified Controlled Nuclear Information (UCNI), National Disclosure Policy (NDP-1), and cover and cover support information. When warranted, it can be applied to unclassified information properly categorized as CUI having a licensing or export control requirement. Before marking a document or material as NOFORN or NF, it will be reviewed by the Foreign Disclosure Officer to ensure there are no agreements in place to prohibit its use and sharing.

(3) The application of "Releasable to" ("REL TO") can only be applied, when warranted and consistent with relevant law, regulation, or government-wide policy or DoD policy, to information properly categorized as CUI with an export control or licensing requirement with a foreign disclosure agreement in place.

(a) Export-controlled CUI transfers to foreign persons must be in accordance with the Arms Export Control Act, International Traffic in Arms Regulations, Export Control Reform Act, Export Administration Regulations, and DoDI 2040.02. In accordance with DoDDs 5230.11 and 5230.20, a positive foreign disclosure decision must be made before CUI is released to a foreign entity.

(b) DoD operational CUI (not related to intelligence) may be marked as REL TO.

e. All classified documents, including legacy documents will be reviewed for CUI and properly marked upon changes in the document's classification level, particularly if the documents are to be completely declassified.

f. The first page or cover of any document or material containing CUI, including a document with commingled classified information, will include a CUI designation indicator, as shown in Figure 2. This CUI designation indicator is similar to the classification-marking block used for CNSI documents and materials. Documents and materials containing CUI will require a generic "CUI" marking at the top and bottom of each page.

(1) In accordance with Part 2002 of Title 32, CFR, the CUI designation indicator must contain, at minimum, the name of the DoD Component determining that the information is CUI. If letterhead or another standard indicator of origination is used, this line may be omitted.

(2) The second line must identify the office making the determination.

(3) The third line must identify all types of CUI contained in the document.

(4) The fourth line must contain the distribution statement or the dissemination controls applicable to the document.

(5) The fifth line must contain the phone number or office mailbox for the originating DoD Component or authorized CUI holder.

Figure 2. CUI Designation Indicator for All Documents and Material

Controlled by: [Name of DoD Component] (Only if not on letterhead)
Controlled by: [Name of Office]
CUI Category: (List category or categories of CUI)
Distribution/Dissemination Control:
POC: [Phone or email address]

g. During DoD's initial phased implementation of the CUI Program, there is no required distinction that must be made between Basic and Specified CUI. All DoD information will be protected in accordance with the requirements under the Basic level of safeguards and dissemination unless specifically identified otherwise in a law, regulation, or government-wide policy. Forthcoming guidance will address the distinction between the two levels of CUI, including a list of which categories are Basic or Specified, what makes the category one or the other, and the unique requirements, to include markings, for each.

3.5. GENERAL DOD CUI ADMINISTRATIVE REQUIREMENTS.

Each DoD Component head must appoint, in writing, a CSAO for the Information Security Program, who will:

a. Appoint, in writing, an official to serve as the CPM for CUI in accordance with ISSO Notice 2019-02. To manage the DoD Component's overall execution of the CUI program, the CPM will:

(1) Coordinate directly with the USD(I&S) Information Security Directorate on CUI matters.

(2) Manage and oversee CUI implementation for the DoD Component.

(3) Inform the CSAO of concerns identified by subordinate elements.

(4) Report misuse, mishandling, or UD of CUI to the Unauthorized Disclosure Program Management Office. In addition, notify the appropriate Military Department Counterintelligence Organization of all incidents.

(5) Submit the annual CUI Implementation Status Report to the DDI(CL&S) to evaluate the effectiveness, compliance, and efficiency of the DoD Component's implementation of CUI, in accordance with Paragraph 3.6.c.

(6) Resolve CUI challenges in accordance with E.O. 13556 and Part 2002 of Title 32, CFR. Refer all unresolved challenges to the DDI(CL&S).

b. Serve as the primary point of contact for official correspondence, accountability reporting, and other matters of record between the DoD Component and the USD(I&S).

3.6. GENERAL DOD CUI PROCEDURES.

DoD CUI is clustered into organizational indexes (e.g., defense, privacy, proprietary) with associated categories, and is categorized by the DoD according to the specific law, regulation, or government-wide policy requiring control. Unclassified information associated with a law, regulation, or government-wide policy and identified as needing safeguarding is considered CUI. It requires access control, handling, marking, dissemination controls, and other protective measures for safeguarding.

a. The authorized holder of a document or material is responsible for determining, at the time of creation, whether information in a document or material falls into a CUI category. If so, the authorized holder is responsible for applying CUI markings and dissemination instructions accordingly.

b. In accordance with this issuance, every individual at every level, including DoD civilian and military personnel as well as contractors providing support to the DoD pursuant to

contractual requirements, will comply with the requirements in Paragraph 3.6.f of this issuance for initial and annual refresher CUI training.

c. Each OSD and DoD Component will annually submit the CUI Implementation Status Report to the USD(I&S) for inclusion in the DoD CUI Program report to the CUI EA. A copy of the report will be made available on Intelink at https://intelshare.intelink.gov/sites/ousdi/hcis/sec/icdirect/information/CUI/Forms/AllItems.aspx. The CUI Implementation Status Report will at least include:

(1) Implementation activities.

(2) Training statistics.

(3) Incident management.

(4) Implementation and sustainment costs.

(5) Self-inspection activities.

d. DoD and OSD Components will submit an initial report on the implementation status of their CUI Programs. Once established, DoD Component heads will conduct inspections of their programs, and the DoD Implementation Status Report will transition to an annual self-inspection report.

e. Some documents and materials containing CUI may constitute permanently valuable government records and will be maintained and disposed of in accordance with the NARA-approved record disposition schedules applicable to each DoD Component in accordance with DoDI 5015.02. When other materials containing CUI no longer require safeguarding, they will be decontrolled and either retained, if a permanent record, or destroyed in accordance with Section 4 and ISOO Notice 2019-03.

f. Other Executive Branch Agencies in the U.S. Government have identified organizational indexes and CUI categories related to a law, regulation, or government-wide policy. Some CUI indexes and categories are unique to specific organizations. The Official CUI Registry is on the NARA Website at https://www.archives.gov/cui. It identifies other CUI categories not specific to the Defense Index, but that may apply or relate to the Executive Branch. Since various DoD Components interact and share inter-dependencies with other departments, agencies, and activities in the Executive Branch, it is important to know and understand these indexes and categories, along with their associated markings, in order to recognize other agencies' CUI and handle the information accordingly. Of note, the CUI indexes and categories listed in the CUI Registry and DoD CUI Registry identify the safeguarding and dissemination requirements as identified by the related law, regulation, or government-wide policy. Moreover, the CUI Registry is agile and subject to change based on changes in law, regulation, or government-wide policy.

g. In accordance with ISOO Notice 2016-01, CUI training standards must, at minimum:

(1) Identify individual responsibilities for protecting CUI.

(2) Identify the organizational index with CUI categories routinely handled by DoD personnel.

(3) Describe the CUI Registry, including purpose, structure, and location (http://www.archives.gov/cui).

(4) Describe the differences between CUI Basic and CUI Specified.

(5) Identify the offices or organizations with DoD CUI Program oversight responsibilities.

(6) Address CUI marking requirements as described in this issuance.

(7) Address the required physical safeguards and CUI protection methods as described in this issuance.

(8) Address the destruction requirements and methods as described in this issuance.

(9) Address the incident reporting procedures as described in this issuance.

(10) Address methods for properly disseminating CUI within the DoD and with external entities inside and outside of the Executive Branch.

(11) Address the methods for properly decontrolling CUI as described in this issuance.

3.7. GENERAL DOD CUI REQUIREMENTS.

This section specifies initial requirements for implementing, marking, and managing the CUI program. Table 1 contains a sample list of the categories found in the DoD CUI Registry and Defense Index. A complete list of CUI Indexes and Categories can be found on Intelink at https://intelshare.intelink.gov/sites/ousdi/hcis/sec/icdirect/information/CUI/Forms/AllItems.aspx. Some significant points about DoD CUI include:

a. CUI does not include information lawfully and publicly available without restrictions.

b. CUI requires safeguarding measures identified by the CUI EA in Part 2002.14 of Title 32, CFR and, as necessary, in the law, regulation, or government-wide policy with which it is associated. DoD CUI may be disseminated to DoD personnel to conduct official DoD and U.S. Government business in accordance with a law, regulation, or government-wide policy.

(1) No individual may have access to CUI information unless it is determined he or she has an authorized, lawful government purpose.

(2) The person with authorized possession, knowledge, or control of CUI will determine whether an individual has an authorized, lawful government purpose to access designated CUI.

(3) CUI information may be disseminated within the DoD Components and between DoD Component officials and DoD contractors, consultants, and grantees to conduct official

business for the DoD, provided dissemination is consistent with controls imposed by a distribution statement or limited dissemination controls (LDC).

(4) CUI designated information may be disseminated to a foreign recipient in order to conduct official business for the DoD, provided the dissemination has been approved by a disclosure authority in accordance with Paragraph 3.4.c. and the CUI is appropriately marked as releasable to the intended foreign recipient.

c. CTI compiled or aggregated may become classified. Such classified CTI is subject to the requirements of the National Industrial Security Program, which has different requirements than Section 252.204-7012 of the DFARS for unclassified CTI.

(1) CTI is to be marked with one of the Distribution Statements B through F, in accordance with DoDI 5230.24.

(2) Pursuant to section 252.204-7012 of the DFARS, scientific, technical, and engineering information beyond basic research(known as pre-applied research and development aligning with the Science, Technology, and Engineering Information Program policies, with military or space application subject to controls on the access, use, reproduction, modification, performance, transmission, display, release, disclosure, or dissemination) shall be treated as CUI. This type of information or data can become classified by compilation or aggregation and is subject to the National Disclosure Policy (NDP-1). Examples include preliminary research and engineering data, engineering drawings, and associated specifications, lists, standards, process sheets, manuals, technical reports, technical orders, studies and analyses on topics requested by DoD Components, catalog-item identifications, data sets, and computer software with executable or source code.

d. As DoD programs transition through the acquisition life cycle, the CUI category or treatment of information may change. In accordance with Title 32, CFR, if the safeguarding requirements for a CUI category or the original law, regulation, or government-wide policy changes, there will be a cascading effect requiring changes for the particular category. These changes will be implemented as soon as possible.

(1) For example, in the acquisition area, a program will begin in the basic research and development phase. Once this program milestone is achieved, the project could transition to the applied research and development or to the production phase.

(2) At this point, the original CUI must be reviewed for any necessary adjustments, including potential changes to the CUI designation, category, subcategory or type, or controls.

e. CUI will be identified in SCGs to ensure such information receives appropriate protection. If the SCG is canceled, a memorandum or other guidance document may be issued to identify CUI instead.

f. DoD is required to provide documents and records requested by members of the public, unless those records are exempt from disclosure in accordance with the procedures established by Part 286 of Title 32, CFR and DoDD 5400.07.

g. Other CUI category information may qualify for withholding from public release based on a specific FOIA exemption for the type of information in question. Determining whether information meets the requirements for CUI shall be done separately and prior to identifying any potential FOIA exemptions.

h. CUI requiring distribution statements in accordance with DODI 5230.24 or the LDC identified in the related law, regulation, or government-wide policy, but does not qualify as classified information in accordance with E.O. 13526 or Chapter 14 of Title 42, U.S.C, (also known and referred to in this issuance as the "Atomic Energy Act of 1954"), will be implemented in accordance with this issuance.

i. Table 1 is an example of the format for the list of all DoD CUI Registry Categories aligned to the CUI National Registry published on Intelink at https://intelshare.intelink.gov/sites/ousdi/hcis/sec/icdirect/information/CUI/Forms/AllItems.aspx.

j. Table 1 provides a sample of the cross-walk of the National CUI registry to the DoD issuance(s) related to the category. The items in Table 1 identify the two unique types of data used by the Department of Energy, the DoD, and the DoD Components. Both types satisfy the CUI requirements and are subject to safeguarding and limited distribution control, and are exempt from mandatory public disclosure in accordance with Exemption 3 of the FOIA.

Table 1. DoD CUI Registry Category Examples

Category	Proposed Defense Description	Additional Information (How Used, Examples, etc.)	Authority	DoD Guidance	Miscellaneous Information
NNPI	Related to the safety of reactors and associated naval nuclear propulsion plants, and control of radiation and radioactivity associated with naval nuclear propulsion activities, including prescribing and enforcing standards and regulations for these areas as they affect the environment and the safety and health of workers, operators, and the general public. This subcategory of Defense CUI relates to the protection of information concerning nuclear reactors, materials, or security and concerns the safeguarding of nuclear reactors, materials, or security. Refer to Office of the Chief of Naval Operations Instruction N9210.3, and CG-RN-1, Revision 3, Department of Energy-DoD Classification Guide for the Naval Nuclear Propulsion Program for guidance on determining information as Unclassified Defense-NNPI.	Data and information related to the safety of reactors and associated naval nuclear propulsion plants, the control of radiation and radioactivity associated with Defense naval nuclear propulsion activities containing prescriptive and enforcement standards and regulations for these areas as they affect the environment and the safety and health of workers, operators, and the general public.	Section 2013 of Title 42, U.S.C.; Section 2511 of Title 50, U.S.C.	Chief of Naval Operations Instruction N9210.3, and CG-RN-1, Revision 3.	Sanctions: Section 2168 and 2168(b) of Title 42, U.S.C. **The DoD NNPI is unique as it is exempt from mandatory public disclosure under Exemption 3 of the FOIA.**
Unclassified Controlled Nuclear Information - Defense	Relating to Department of Defense special nuclear material (SNM), equipment, and facilities, as defined by Part 223 of Title 32, CFR. This type of Defense CUI is unclassified information about SNM security measures, DoD SNM equipment, DoD SNM facilities, or nuclear weapons in DoD custody. Information is designated DoD unclassified controlled nuclear information (UCNI) in accordance with DoDI 5210.83 only when it is determined its UD could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of the illegal production of nuclear weapons or the theft, diversion, or sabotage of DoD SNM, DoD SNM equipment, DoD SNM facilities, or nuclear weapons in DoD custody.	This type of Defense CUI may be designated UCNI by the Heads of the DoD Components and individuals delegated authority in accordance with DoDD 5210.83. Some specific examples include: Security plans, procedures, and equipment used for the physical safeguarding of DoD SNM.	Section 128(a) of Title 10, U.S.C.; Part 223 of Title 32, CFR	DoDD 5210.83; DoDI 5210.83;	**The DoD UCNI is unique as it is exempt from mandatory public disclosure under Exemption 3 of the FOIA.**

k. Restricted data or formerly restricted data are classified and shall not be commingled with CUI in an unclassified document. For restricted data or formerly restricted data, follow the marking requirements in accordance with Volume 2 of DoDM 5200.01; Part 1045 of Title 10, CFR; and the Atomic Energy Act of 1954.

l. For DoD Geospatial intelligence information and data, the DoD will not apply the Geodetic Product Information (GPI) designation. Instead, the DoD will continue to use the designation for "Limited Distribution" with the marking of "LIMDIS." For all other DoD geospatial information and data, such as installation geospatial information and services (IGI&S) as defined by DoDI 8130.01, use the GPI category or other appropriate CUI category designations defined by this issuance. The DoD will use the GPI designation for all of the non-Geospatial intelligence information and data. Approved LDCs for the DoD are located on Intelink at https://intelshare.intelink.gov/sites/ousdi/hcis/sec/icdirect/information/CUI/Forms/AllItems.aspx.

m. The request for a waiver for a particular CUI Program requirement will be handled in accordance with Volume 1 of DoDM 5200.01 for CNSI.

n. DoD Component heads shall produce annual self-inspection reports and general program status updates to fulfill ISOO monitoring and reporting requirements.

3.8. OCA.

DoD OCAs will determine if CUI under their control, when compiled, is classified. If so, the applicable SCGs must address the compilation. Any time an OCA discovers that compiled or aggregated information is not properly classified on websites, folders, or documents, the OCA will:

a. Notify the organization using the compiled information to remove or protect the information.

b. Conduct a damage assessment.

c. Determine if the information still requires classified protection in its compiled form. If not, the OCA must document the revised aggregation or compilation determination by updating SCGs and providing the guide to all users in accordance with DoDM 5200.45.

d. If the information is determined not to be classified, it must be reviewed to identify if the information is CUI.

e. Since OCAs are the owners of the information under their authority, they are authorized to identify and mark such information as CUI.

3.9. GENERAL RELEASE AND DISCLOSURE REQUIREMENTS.

a. The release or disclosure to foreign governments, international organizations, coalitions, or allied personnel of CUI not controlled as NOFORN will be in accordance with a law, regulation, or government-wide policy. Access to such CUI during official foreign national visits and assignments to DoD Components and cleared contractor facilities, when applied by contract, will be in accordance with DoDD 5230.20.

b. CUI not controlled as NOFORN may be released or disclosed to non-U.S. citizens employed by the DoD if:

(1) Access to such information is within the scope of their assigned duties.

(2) Access to such information would help accomplish a lawful and authorized DoD mission or purpose and would not be detrimental to the interests of the DoD or the U.S. Government.

(3) There are no contract restrictions prohibiting access to such information.

(4) Access to such information is in accordance with DoDIs 8500.01 and 5200.02 and export control regulations, as applicable.

c. The DoD Components' CSAOs and CPMs 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.

d. For UD of CUI, no formal security inquiry or investigation is required unless disciplinary action will be taken against the individual(s) responsible. In such cases, a preliminary inquiry is appropriate. 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 law, regulation, or government-wide policy. The DoD Component originating the CUI will be informed of any UD.

e. Reporting or accounting for UD of CUI shall be done in accordance with Paragraph 3.5.a(4), and the appropriate Military Department Counterintelligence Organization shall be notified of all incidents.

3.10. GENERAL SYSTEM AND NETWORK CUI REQUIREMENTS.

In accordance with DoDIs 8500.01 and 8510.01, security controls for systems and networks are set to the level required by the safeguarding requirements for the data or information being processed, as identified in Federal Information Processing Standards 199 and 200. For DoD CUI, the minimum security level will be moderate confidentiality in accordance with Part 2002 of Title 32, CFR and NIST SP 800-171.

a. The USD(I&S) will notify and coordinate with the CUI EA regarding waiver requests involving CUI requirements prior to granting any such requests, including waiver requests

related to IS. The USD(I&S) must coordinate and collaborate with the DoD CIO to ensure the agency requesting the waiver has plans to appropriately safeguard and control CUI. The request for a waiver for a CUI Program requirement shall be done in accordance with Volume 1 of DoDM 5200.01 for CNSI, as modified in the forthcoming manual supporting this instruction.

b. DoD personnel will not use unofficial or personal (e.g., .net; .com) e-mail accounts, messaging systems, or other non-DoD information systems, except approved or authorized government contractor systems, to conduct official business involving CUI. This is necessary to ensure proper accountability for Federal records and to facilitate data spill remediation in accordance with Public Law 113-187 and the January 16, 2018 Deputy Secretary of Defense memorandum.

c. DoD information systems processing, storing, or transmitting CUI will be categorized at the moderate impact level, and follow the guidance in DoDIs 8500.01 and 8510.01. Non-DoD information systems processing, storing, or transmitting CUI will provide adequate security, and the appropriate requirements must be incorporated into all contacts, grants, and other legal agreements with non-DoD entities in accordance with DoDI 8582.01. The NIST SP 800-171 governs and protects CUI on non-Federal IS when applied by contract.

d. For systems, networks, and programs operating on the various domains, a splash screen warning and notice of consent, as shown in Figure 3, must be employed to alert users of CUI within the program. This ensures proper safeguarding and dissemination controls are implemented in accordance with Part 2002 of Title 32, CFR and this issuance.

Figure 3. Notice and Consent

"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

e. Organizations will modify or install classification marking tools on UNCLASSIFIED, SECRET, and TOP SECRET network systems to account for CUI information and readily permit inclusion of CUI markings and designator indicators as required by Part 2002 of Title 32, CFR.

SECTION 4: DISSEMINATION, DECONTROLLING, AND DESTRUCTION OF CUI

4.1. GENERAL.

Part 2002 of Title 32, CFR requires dissemination statements to be placed on classified and unclassified documents or other materials when CUI necessitates access restrictions, including those required by law, regulation, or government-wide policy. These statements facilitate control, secondary sharing, decontrol, and release without the need to repeatedly obtain approval or authorization from the controlling DoD office.

a. Dissemination controls identify the audience deemed to have a lawful government purpose to use the CUI and specify the rationale for applying the controls by specific codes in accordance with DoDI 5230.24 and this issuance.

b. Agencies must promptly decontrol CUI properly determined by the CUI owner to no longer require safeguarding or dissemination controls, unless doing so conflicts with the related law, regulation, or government-wide policy in accordance with DoDI 5230.09.

c. Decontrolling CUI through the public release process relieves authorized holders from requirements for handling information in accordance with the CUI Program. A prepublication review must be conducted in accordance with DoDI 5230.09 before public release may be authorized.

d. In accordance with Part 2002.20 of Title 32, CFR, if the authorized holder of the CUI publicly releases the CUI in accordance with the designating agency's authorized procedures, this constitutes the decontrol of the document.

e. To ensure CUI protection, the following measures will be implemented:

(1) 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. The concept of a controlled environment means there is sufficient internal security measures in place to prevent or detect unauthorized access to CUI. For DoD, an open storage environment meets these requirements.

(2) CUI information and material may be transmitted via first class mail, parcel post, or, bulk shipments. When practical, CUI information may be transmitted electronically (e.g., data, website, or e-mail), via approved secure communications systems or systems utilizing other protective measures such as Public Key Infrastructure or transport layer security (e.g., https). Avoid wireless telephone transmission of CUI when other options are available. CUI transmission via facsimile machine is permitted; however, the sender is responsible for

determining whether appropriate protection will be available at the receiving location before transmission (e.g., facsimile machine attended by a person authorized to receive CUI; facsimile machine located in a controlled government environment).

4.2. DISSEMINATION REQUIREMENTS FOR DOD CUI.

a. In accordance with this issuance, CUI access should be encouraged and permitted to the extent the access or dissemination:

(1) Complies with the law, regulation, or government-wide policy identifying the information as CUI.

(2) Furthers a lawful government purpose.

(3) Is not restricted by an authorized LDC established by the CUI EA.

(4) Is not otherwise prohibited by any other law, regulation, or government-wide policy.

b. Agencies may place limits on disseminating CUI for a lawful government purpose only using the dissemination controls listed in Table 2 or methods authorized by a specific law, regulation, or government-wide policy.

c. When handling other Executive Branch CUI, DoD personnel will follow their governance criteria for when the application of dissemination controls and its markings are allowed, and by whom, while ensuring the policy is in accordance with Part 2002 of Title 32, CFR.

d. LDCs or distribution statements cannot unnecessarily restrict CUI access.

e. Since DoD Components need to retain certain agency-specific CUI within their organizations, DoD Components may use the limited dissemination controls to limit access to those on an accompanying dissemination list, as shown in Table 2. For example, raw data, information, or products must be processed and analyzed before determining if further dissemination is required or permitted. The Limited Dissemination Control List control will be used to address this need. The LDC list is found on Intelink at https://intelshare.intelink.gov/sites/ousdi/hcis/sec/icdirect/information/CUI/Forms/AllItems.aspx.

4.3. LEGACY DISTRIBUTION STATEMENTS.

a. Legacy CUI technical documents and materials requiring export control have used distribution statements in accordance with DoDI 5230.24 in order to address the shared responsibility between the DoD and its contractors to safeguard this information. This was done for legacy CUI creation, transmission, receipt, storage, distribution, decontrol, and approved disposition authorities, including destruction.

b. As of the effective date of this issuance, DoD personnel will use LDCs for new CUI documents and materials except export controlled technical information, which must be marked

with an export control warning in accordance with DoDI 5230.24, DoDD 5230.25, and Part 250 of Title 32, CFR. The wording of the distribution statements may not be modified to specify additional distribution, such as distribution to foreign governments. However, where other markings are authorized and used in accordance with associated law, regulation, or government-wide policy (e.g., North Atlantic Treaty Organization markings, REL TO), those markings may be used to further inform distribution decisions. Therefore, "REL TO" is authorized for use with foreign nationals once the information distribution is properly coordinated with the foreign disclosure office.

Table 2. Dissemination Control and Distribution Statement Markings

NEW LDC	ALIGNMENT TO CURRENT
NONE – Publicly Releasable **AFTER** Review	DISTRO A
No Foreign Dissemination (NOFORN / NF)	
Federal Employees Only (FED ONLY)	DISTRO B
Federal Employees and Contractors Only (FEDCON)	DISTRO C
No Dissemination to Contractors (NOCON)	
Dissemination List Controlled (DL ONLY)	DISTRO F
Authorized for Release to Certain Foreign Nationals Only (REL TO USA, LIST)	
Display Only (DISPLAY ONLY)	
Dissemination List – (Include Separate List for Government Only)*	DISTRO E
Dissemination List – (Include Separate List for Government and Contractors Only)*	DISTRO D
NONE	DISTRO X: U.S. Government Agencies and private individuals or enterprises eligible to obtain export controlled technical data in accordance with DoDD 5230.25. DISTRO X was cancelled and superseded by DISTRO C.
*The dissemination list limits access to the specified individuals, groups, or agencies and must accompany the document	

c. CUI export controlled technical information or other scientific, technical, and engineering information will still use distribution statements. Export controlled information must also be marked with an export control warning as directed in DoDI 5230.24, DoDD 5230.25, and Part 250 of Title 32, CFR.

4.4. DECONTROLLING.

Guidance for decontrolling CUI records, documents, and materials is provided in this issuance, or the CUI Registry for information categories not directly related to DoD CUI.

a. CUI documents and materials will be formally reviewed in accordance with DoDI 5230.09 before being decontrolled or released to the public.

b. The originator or other competent authority (e.g., initial FOIA denial and appellate authorities) will terminate the CUI status of specific information when the information no longer requires protection from public disclosure. When the CUI status of information is terminated in this manner, all known holders will be notified by email or other means. Upon notification, holders will remove the CUI markings. Holders will not need to retrieve records on file solely for this purpose. Information with a terminated CUI status will not be publicly released without review and approval in accordance with DoDIs 5230.09, 5230.29, and 5400.04.

4.5. DESTRUCTION.

Guidance for destroying CUI documents and materials is provided in this issuance, the CUI Registry, and ISOO Notice 2019-03. CUI documents and materials will be formally reviewed in accordance with Paragraphs 4.5.a. and 4.5.b. before approved disposition authorities are applied, including destruction. Media containing CUI must include decontrolling indicators.

a. Record and non-record copies of CUI documents will be disposed of in accordance with Chapter 33 of Title 44, U.S.C. and the DoD Components' records management directives. When destroying CUI, including in electronic form, agencies must do so in a manner making it unreadable, indecipherable, and irrecoverable. If the law, regulation, or government-wide policy specifies a method of destruction, agencies must use the method prescribed.

b. 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 unrecoverable the original information such as those identified in NIST SP 800-88 and in accordance with Section 2002.14 of Title 32, CFR.

SECTION 5: APPLICATION OF DOD INDUSTRY

5.1. GENERAL.

There is a shared responsibility between the DoD and industry, when established by contract, grants, or other legal agreements or arrangements, in the identification, creation, sharing, marking, safeguarding, storage, dissemination, decontrol, disposition, destruction, and records management of CUI documents and materials. It is essential to identify and apply the general dissemination principles and guidance as prescribed by the CUI EA in accordance with Part 2002 of Title 32, CFR. Contracts containing CUI shared from DoD or generated, managed, or transmitted by the contractor via their information systems, will be in accordance with this issuance, which will be incorporated into each DoD contract.

a. The NIST SP 800-171 identifies the baseline CUI system security requirements for industry established by Part 2002 of Title 32, CFR. Additionally, Section 252.204-7012 of the DFARS specifies a waiver process for defense contractors in accordance with NIST SP 800-171 for contractor IT or networks.

b. CUI with the potential to impact national security (e.g., information related to critical programs and technology information) may require enhanced protection. These enhanced measures would address both physical and logical procedures. Enhanced protection methods for systems hosting CUI include:

(1) Access control (e.g., restricting both physical and logical access to the systems).

(2) Audit and accountability (e.g., review and monitor system usage).

(3) Configuration management (e.g., restrict system connection to only approved resources).

(4) Identification and authentication (e.g., control issuance of end-user certificates).

(5) Incident response (e.g., ensure corrective measures are implemented in a timely manner and validate effectiveness).

(6) System and communication protection (e.g., application of encryption for data at rest and restriction of connections to uncertified, unsecured, non-organizational systems). DoD Components may implement stricter CUI encryption requirements based on a law, regulation, or government-wide policy (DHA PI 8140, requires workforce encrypt emailed PHI).

(7) System and information integrity (e.g., provide network detection tools throughout the system to identify attempted intrusions).

c. Non-DoD IS processing, storing, or transmitting CUI will be safeguarded in accordance with contractual requirements identified for the particular CUI contained in the contract, DoDI 8582.01 and Section 252.204-7012 of the DFARS or their subsequent revisions.

d. When established by contract, contractors, sub-contractors, and consultants must comply with safeguarding requirements identified in the contract for all types of CUI.

e. The program office or requiring activity must identify DoD CUI at the time of contract award and, if necessary, provide guidance on information aggregation or compilation. The program office or requiring activity must review recurring or renewed contracts for CUI to comply with this issuance.

5.2. MISUSE OR UD OF CUI.

Safeguarding requirements and incident response measures for misuse or UD of CUI must be implemented across the DoD. Senior leaders, contracting officers, commanders, and supervisors at all levels must consider and take appropriate administrative, legal, or other corrective or disciplinary action to address CUI misuse or UD commensurate with the appropriate law, regulation, or government-wide policy.

5.3. REQUIREMENTS FOR DOD CONTRACTORS.

This paragraph highlights requirements for DoD contractors.

a. Whenever DoD provides information to contractors, it must identify whether any of the information is CUI via the contracting vehicle, in whole or part, and mark such documents, material, or media in accordance with this issuance.

b. Whenever the DoD provides CUI to, or CUI is generated by, non-DoD entities, protective measures and dissemination controls, including those directed by relevant law, regulation, or government-wide policy, will be articulated in the contract, grant, or other legal agreement, as appropriate.

c. DoD contracts must require contractors to monitor CUI for aggregation and compilation based on the potential to generate classified information pursuant to security classification guidance addressing the accumulation of unclassified data or information. DoD contracts shall require contractors to report the potential classification of aggregated or compiled CUI to a DoD representative.

d. DoD personnel and contractors, pursuant to mandatory DoD contract provisions, will submit unclassified DoD information for review and approval for release in accordance with the standard DoD Component processes and DoDI 5230.09.

e. All CUI records must follow the approved mandatory disposition authorities whenever the DoD provides CUI to, or CUI is generated by, non-DoD entities in accordance with Section 1220-1236 of Title 36, CFR, Section 3301a of Title 44, U.S.C., and this issuance.

GLOSSARY

G.1. ACRONYMS.

ACRONYM	MEANING
CFR	Code of Federal Regulations
CMO	Chief Management Officer of the Department of Defense
CNSI	classified national security information
CPM	Component program manager
CSAO	Component senior agency official
CTI	controlled technical information
CUI	controlled unclassified information
DDI(CL&S)	Director For Defense Intelligence (Counterintelligence, Law Enforcement, And Security)
DCSA	Defense Counterintelligence and Security Agency
DFARS	Defense Federal Acquisition Regulation Supplement
DNI	Director of National Intelligence
DoD CIO	Department of Defense Chief Information Officer
DoDD	DoD directive
DoDI	DoD instruction
DoDM	DoD manual
EA	Executive Agent
E.O.	Executive order
FOIA	Freedom of Information Act
GPI	Geodetic Product Information
ISOO	Information Security Oversight Office
IS	information systems
LDC	limited dissemination controls
NARA	National Archives and Records Administration
NISP	National Industrial Security Program
NIST SP	National Institute of Standards and Technology Special Publication
NNPI	Naval Nuclear Propulsion Information
NOFORN or NF	not releasable to foreign nationals
OCA	original classification authority
OIG DoD	Office of the Inspector General of the Department of Defense
PFPA	Pentagon Force Protection Agency

ACRONYM	MEANING
REL TO	releasable to
SCG	security classification guide
SNM	special nuclear material
U	Unclassified information
UCNI	unclassified controlled nuclear information
UD	unauthorized disclosure
U.S.C.	United States Code
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment
USD(I&S)	Under Secretary of Defense for Intelligence and Security
USD(R&E)	Under Secretary of Defense for Research and Engineering

G.2. DEFINITIONS.

Unless otherwise noted, these terms and their definitions are for the purpose of this issuance. Referenced definitions related to CUI in Section 2002.4 of Title 32, CFR can be found at https://intelshare.intelink.gov/sites/ousdi/hcis/sec/icdirect/information/CUI/Forms/AllItems.aspx.

TERM	DEFINITION
access	The ability or opportunity to acquire, examine, or retrieve CUI.
agency	Defined in Section 2002.4 of 32 CFR
aggregation	The creation of classified information from the accumulation of unclassified data or information from several areas within a document.
agreements and arrangements	Defined in Section 2002.4 of Title 32 CFR
authorized CUI holder	Defined in Section 2002.4 of Title 32 CFR
classified information	Defined in Section 2002.4 of Title 32 CFR
compilation	The creation of classified information resulting from the accumulation of unclassified data or information from several documents.

TERM	DEFINITION
contract	Defined in Section 252.204- 2008 and 7012 of the FARS/DFARS.
controlled environment	Defined in Section 2002.4 of Title 32 CFR
controls	Defined in Section 2002.4 of Title 32 CFR
CNSI	Defined in E.O. 13526.
CPM	Defined in Section 2002.4 of Title 32 CFR
CSAO	An official designated, in writing, by a DoD Component head who is responsible to the agency head for implementing the CUI Program. Also known as CUI SAO as defined in Section 2002.4 of Title 32 CFR
CTI	Defined in the DFARS 204.7301.
CUI	Defined in Section 2002.4 of Title 32 CFR
CUI Basic	Defined in Section 2002.4 of Title 32 CFR (DoD is not using this structure in its initial implementation phase.)
CUI category	Defined in Section 2002.4 of Title 32 CFR
CUI EA	Defined in Section 2002.4 of Title 32 CFR
CUI Indexes	An organizational grouping of CUI categories as defined by the CUI EA. The term was created by the CUI EA to replace the notion of a sub-category which implies a hierarchy structure or importance.
CUI misuse	Use of CUI in a manner not in accordance with the policy contained in E.O. 13556; Part 2002 of Title 32, CFR; the CUI Registry; agency CUI policy; or the applicable LRGWP governing the information.
CUI Program	Defined in Section 2002.4 of Title 32 CFR
CUI Registry	Defined in Section 2002.4 of Title 32 CFR
CUI Specified	Defined in Section 2002.4 of Title 32 CFR (DoD is not using this structure in its initial implementation phase.)
decontrol	Defined in Section 2002.18 of Title 32, CFR.

TERM	DEFINITION
Defense Industrial Base	Defined in the DoD Dictionary of Military and Associated Terms.
disseminating	Defined in Section 2002.4 of Title 32 CFR
document	Defined in Section 2002.4 of Title 32 CFR
DoD personnel	Defined in DoDI 5230.09.
foreign entity	Defined in Section 2002.4 of Title 32 CFR
formerly restricted data	Defined in Section 1045 of Title 10, CFR.
handling	Defined in Section 2002.4 of Title 32 CFR
lawful government purpose	Defined in Section 2002.4 of Title 32 CFR
LDC	Defined in Section 2002.4 of Title 32 CFR
legacy material	Defined in Section 2002.4 of Title 32 CFR
Limited Distribution	A legacy CUI category used by the National Geospatial-Intelligence Agency to identify a select group of sensitive, unclassified imagery or geospatial information and data created or distributed by National Geospatial Intelligence Agency or information, data, and products derived from such information (marked as LIMDIS and now referred to a GPI by CUI EA).
logical access	Electronic access controls authenticated through outside certificates accepted by the DoD to limit access to data files and systems only by vetted individuals.
misuse	Defined in Section 2002.4 of Title 32 CFR
NNPI	Information concerning the design, arrangement, development, testing, operation, administration, training, maintenance, and repair of the propulsion plants of naval nuclear powered ships and prototypes, including the associated nuclear support facilities.
non-Executive Branch entity	Defined in Section 2002.4 of Title 32 CFR

TERM	DEFINITION
personally identifiable information	Defined in Office of Management and Budget Circular No. A-130.
physical access	All DoD and non-DoD personnel entering or exiting DoD facilities or installations that authenticated a physical access control system (PACS).
portion	Defined in Section 2002.4 of Title 32 CFR
protection	Defined in Section 2002.4 of Title 32 CFR
public release	Defined in Section 2002.4 of Title 32 CFR
records	Defined in Section 2002.4 of Title 32 CFR
restricted data	Defined in Part 1045 of Title 10, CFR.
re-use	Defined in Section 2002.4 of Title 32 CFR
safeguarding	Prescribed measures and controls that protect classified information and CUI.
Senior Agency Official	An official appointed by the Secretary of Defense to be responsible for direction, administration, and oversight of the DoD's Information Security Program, including classification, declassification, CUI, safeguarding, and security education and training programs, and for the efficient and effective implementation of the guidance in this issuance.
SCG	Security classification guidance issued by an OCA identifying the elements of information regarding a specific subject requiring classification, and establishes the level and duration of classification for each element.
self-inspection	Defined in Section 2002.4 of Title 32 CFR
UD	Defined in Section 2002.4 of Title 32 CFR
unclassified	Information not requiring control, but requiring review before public release.

REFERENCES

Code of Federal Regulations, Title 10, Part 1045

Code of Federal Regulations, Title 32

Code of Federal Regulations, Title 36

Defense Federal Acquisition Regulation Supplement, Subparts 252.204-2008 and 7012, current edition

Deputy Secretary of Defense Memorandum, "Designation of Senior Agency Official for Controlled Unclassified Information," December 22, 2010

Deputy Secretary of Defense Memorandum, "Unauthorized Disclosures of Classified Information or Controlled Unclassified Information on DoD Information Systems," August 14, 2014

DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I))," October 24, 2014, as amended

DoD Directive 5200.43, "Management of the Defense Security Enterprise," October 01, 2012, as amended

DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations (NDP-1)," June 16, 1992

DoD Directive 5230.20, "Visits and Assignments of Foreign Nationals," June 22, 2005

DoD Directive 5400.07, "DoD Freedom of Information Act (FOIA) Program," April 5, 2019

DoD Instruction 2040.02, "International Transfers of Technology, Articles, and Services," March 27, 2014, as amended

DoD Instruction 3200.12, "DoD Scientific and Technical Information Program (STIP)," August 22, 2013, as amended

DoD Instruction 5015.02, "DoD Records Management Program," February 24, 2015, as amended

DoD Instruction 5200.02, "DoD Personnel Security Program (PSP), Change 2," March 21, 2014, as amended

DoD Instruction 5210.83, "DoD Unclassified Controlled Nuclear Information (UCNI)," July 12, 2012, as amended

DoD Instruction 5230.09, "Clearance of DoD Information for Public Release," January 25, 2019

DoD Instruction 5230.24, "Distribution Statements on Technical Documents," August 23, 2012, as amended

DoD Instruction 5230.29, "Security and Policy Review of DoD Information for Public Release," August 13, 2014, as amended

DoD Instruction 5400.04, "Provision of Information to Congress," March 17, 2009

DoD Instruction 5400.11, "DoD Privacy and Civil Liberties Programs," January 29, 2019

DoD Instruction 8320.07, "Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense," August 03, 2015, as amended

DoD Instruction 8500.01, "Cybersecurity," March 14, 2014, as amended

DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014, as amended

DoD Manual 5200.01, Volume 1, "DoD Information Security Program: Overview, Classification, And Declassification," February 24, 2012, as amended

DoD Manual 5200.01, Volume 2, "DoD Information Security Program: Marking of Information," February 24, 2012, as amended

DoD Manual 5200.45, "Instruction for Developing Security Classification Guides," April 02, 2013, as amended

DoD Manual 5400.07, "DoD Freedom of Information Act (FOIA) Program," January 25, 2017

Executive Order 13526, "Classified National Security Information," December 29, 2009

Executive Order 13556, "Controlled Unclassified Information," November 04, 2010

Federal Information Processing Standards Publication 199, "Standards for Security Categorization of Federal Information and Information Systems," February 2004

Federal Information Processing Standards Publication 200, "Minimum Security Requirements for Federal Information and Information Systems," March 2006

Information Security Oversight Office, "CUI Notice 2016-01: Implementation Guidance for the Controlled Unclassified Information Program," September 14, 2016

Information Security Oversight Office, "CUI Notice: Decontrolling Controlled Unclassified

Information (CUI) in Response to a Freedom of Information Act (FOIA) Request,"

November 19, 2018

Information Security Oversight Office, "CUI Notice 2019-01: Controlled Unclassified Information (CUI) Coversheets and Labels," February 22, 2019

Information Security Oversight Office, "CUI Notice 2019-02: CUI Program Manage Position Description Template," May 13, 2019

Information Security Oversight Office, "CUI Notice 2019-03: Destroying Controlled Unclassified Information (CUI)," July 15, 2019

Information Security Oversight Office Response Letter to Under Secretary of Defense for Intelligence and Security, August 21, 2019

Information Security Oversight Office Response Letter to Under Secretary of Defense for Intelligence, Subject: "Unclassified versus Uncontrolled Unclassified Information", June 4, 2019

Intelligence Community Directive 710, "Classification Management and Control Markings System," June 21, 2013

Intelligence Community Policy Guidance 403.1, "Criteria for Foreign Disclosure and release of Classified National Intelligence," June 21, 2013

National Institute of Standards and Technology Special Publication 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations," January 14, 2016, as amended

National Institute of Standards and Technology Special Publication 800-88, Revision 1, "Guidelines for Media Sanitization," February 5, 2015

National Strategy for Information Sharing and Safeguarding, December 19, 2012

Office of the Chairman of the Joint Chiefs of Staff, "DoD Dictionary of Military and Associated Terms," current edition

Office of the Chief of Naval Operations Instruction N9210.3, "Safeguarding of Naval Nuclear Propulsion Information (NNPI)," June 7, 2010

Office of Management and Budget Circular No. A-130, "Managing Information as a Strategic Resource," July 28, 2016

OPNAVINST N9210.3, "Safeguarding of Naval Nuclear Propulsion Information (NNPI)", June 07, 2010

Under Secretary of Defense for Intelligence Memorandum, "Controlled Unclassified Information Implementation and Oversight for the Defense Industrial Base," May 17, 2018

United States Code, Title 5

United States Code, Title 10

United States Code, Title 42, Chapter 14 (also known as the "Atomic Energy Act of 1954")

United States Code, Title 44

DoD Instruction 8582.01

Security of Non-DoD Information Systems Processing Unclassified Nonpublic DoD Information

Originating Component:	Office of the Chief Information Officer of the Department of Defense
Effective:	December 9, 2019
Releasability:	Cleared for public release. Available on the DoD Issuances Website at http://www.esd.whs.mil/DD/.
Reissues and Cancels:	DoD Instruction 8582.01, "Security of Unclassified DoD Information on Non-DoD Information Systems," June 6, 2012
Approved by:	Dana Deasy, DoD Chief Information Officer

Purpose: In accordance with the authority in DoD Directive (DoDD) 5144.02, this issuance establishes policy, assigns responsibilities, and provides direction for managing the security of non-DoD information systems that process, store, or transmit unclassified nonpublic DoD information, including controlled unclassified information (CUI).

TABLE OF CONTENTS

TABLES

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY. This issuance:

a. Applies to:

(1) OSD, the Military Departments (including the Coast Guard at all times, including when it is a Service in the Department of Homeland Security by agreement with that Department), the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this issuance as the "DoD Components").

(2) All unclassified non-DoD information systems to the extent provided by applicable contracts, grants, or other legal agreements with the DoD that process, store, or transmit unclassified nonpublic DoD information. This includes unclassified non-DoD information systems operated by mission partners.

b. Does **not** apply to:

(1) DoD information systems operated by a contractor or other entity on behalf of the DoD as described in DoD Instruction (DoDI) 8510.01. Such information systems are treated the same as those operated by a DoD organization.

(2) Non-DoD information systems providing information technology services to the DoD. Such information systems follow the guidance prescribed in DoDIs 8500.01 and 8510.01.

(3) Unclassified DoD information that has been cleared for public release in accordance with DoDD 5230.09.

1.2. POLICY. It is DoD policy that non-DoD information systems provide adequate security for all unclassified nonpublic DoD information. Appropriate requirements must be incorporated into all contracts, grants, and other legal agreements with non-DoD entities, including memorandums of agreement established in accordance with DoDI 4000.19.

SECTION 2: RESPONSIBILITIES

2.1. DOD CHIEF INFORMATION OFFICER (CIO). In addition to the responsibilities in Paragraph 2.5., the DoD CIO:

a. Assigns the DoD Senior Information Security Officer to oversee implementation of this issuance in coordination with the Under Secretary of Defense for Intelligence (USD(I)), the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)), and the Under Secretary of Defense for Research and Engineering (USD(R&E)), as appropriate.

b. Oversees integration of this guidance into Defense Industrial Base (DIB) cybersecurity activities in accordance with DoDI 5205.13.

c. In coordination with the USD(A&S) and the USD(R&E), identifies, develops, and implements the DoD acquisition contracting process, policy, and procedures for improved protection of unclassified DIB information systems where unclassified non-public DoD information is processed, stored, or transmitted on unclassified DIB information systems, to include:

(1) Subsection 52.204-21 of the Federal Acquisition Regulation (FAR).

(2) Subsection 252.204-7012 of the Defense Federal Acquisition Regulation Supplement (DFARS).

d. In coordination with the USD(R&E) and the USD(A&S), engages the DIB to identify and validate best practices to improve protection of nonpublic unclassified DoD information developed, used, and shared by non-DoD entities in support of defense acquisition programs.

e. Requires non-DoD unclassified information systems containing CUI meet the security requirements of Part 2002 of Title 32, Code of Federal Regulations and DoD CUI policy in coordination with the USD(I).

2.2. USD(A&S). In addition to the responsibilities in Paragraph 2.5., the USD(A&S):

a. In coordination with the USD(I), the USD(R&E), the DoD CIO, and the DoD Components, as appropriate, identifies, develops, and implements the acquisition regulations, policies, and procedures for improved protection of contractor information systems processing, storing, or transmitting unclassified DoD information that has not been publicly released.

b. In coordination with the USD(I), the USD(R&E), and the DoD CIO, engages the DIB to identify and validate best practices to improve protection of nonpublic unclassified DoD information developed, used, and shared by non-DoD entities in support of defense acquisition programs.

2.3. USD(R&E). In addition to the responsibilities in Paragraph 2.5., the USD(R&E):

a. In coordination with the DoD CIO and the USD(A&S), engages the DIB to identify and validate best practices to improve protection of nonpublic unclassified DoD information developed, used, and shared by non-DoD entities in support of defense acquisition programs.

b. Develops cyber incident damage assessment policy and oversees the process to conduct assessments of DoD programs, as required, on unauthorized access and compromise of DIB information systems containing unclassified DoD information.

2.4. USD(I). As the DoD Senior Agency Official for Security, the USD(I), in addition to the responsibilities in Paragraph 2.5., in coordination with the DoD CIO, the USD(A&S), and the USD(R&E), as appropriate:

a. Oversees implementation of this issuance in areas of USD(I) responsibility.

b. Ensures information security requirements for CUI contained on non-DoD information systems are in accordance with DoD CUI policy.

2.5. OSD AND DOD COMPONENT HEADS. The OSD and DoD Component heads:

a. Require contracts, grants, or other legal agreements to protect:

(1) Unclassified nonpublic DoD information provided to, or developed by, non-DoD entities in support of DoD activities according to the basic information system safeguards in Table 1 (see Section 3).

(2) DoD CUI provided to, or developed by, non-DoD entities in support of DoD activities according to the DoD CUI information system safeguards described in Paragraph 3.2.b.

b. In addition to the safeguards specified in Section 3, require contracts, grants, and other legal agreements, by the insertion of applicable language, to implement any unique protection measures or reporting requirements regarding compromise, loss, or unauthorized disclosure of DoD CUI required by law, regulation, or government-wide policy (e.g., those relating to privacy, health information, law enforcement, or export control).

c. In accordance with the authority in DoDD 5505.13E, ensure the DoD Cyber Crime Center (DC3) is identified as the single focal point for receiving cyber incident reports from non-DoD entities regarding unclassified information systems of non-DoD entities that process, store, or transmit DoD CUI as described in Paragraph 3.3. Cyber incidents include activities taken through the use of information systems that result in a compromise or an actual or potentially adverse effect on an information system or the information residing therein.

SECTION 3: PROCEDURES

3.1. GENERAL. Unclassified nonpublic DoD information may be disseminated by the contractor, grantee, or awardee to further the contract, grant, or agreement objectives, provided the information is disseminated within the scope of assigned duties, is not otherwise restricted by the contract, grant or agreement, and with a clear expectation that confidentiality will be preserved. Examples are:

a. Nonpublic information provided to a contractor (e.g., with a request for proposal).

b. Information developed during the course of a contract, grant, or other legal agreement (e.g., draft documents, reports, or briefings and deliverables).

c. Privileged information contained in transactions (e.g., privileged contract information, program schedules, or contract-related event tracking).

3.2. INFORMATION SYSTEM SAFEGUARDS. Adequate security will vary depending on the nature and sensitivity of the information on any given non-DoD information system.

a. All non-DoD information systems that process, store, or transmit unclassified nonpublic DoD information must be safeguarded in accordance with the basic safeguarding requirements in Table 1. These requirements must be included in contracts, grants, and other legal agreements (in contracts, these are implemented in accordance with FAR 52.204-21.

b. Non-DoD information systems processing, storing, or transmitting DoD CUI must be protected in accordance with National Institute of Standards and Technology Special Publication (NIST SP) 800-171. If the non-DoD entity intends to use an external cloud service provider to process, store, or transmit any DoD CUI in performance of contracts, grants, or other legal agreements; the non-DoD entity must require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program Moderate baseline (https://www.fedramp.gov/resources/documents/).

(1) This is typically implemented contractually in accordance with DFARS 252.204-7012.

(2) DoD Components should restrict their security requirements to NIST SP 800-171 for information systems processing, storing, or transmitting DoD CUI unless the authorizing law, regulation, or Government-wide policy for the CUI category of the information involved prescribes specific safeguarding requirements for protecting the information's confidentiality, or there is a specific documented need to increase security above the Federal Information Processing Standards Publication 199 moderate impact level.

c. Non-DoD entities meeting the Basic Safeguarding Requirements in Table 1, meet the comparable security requirements of the NIST SP 800-171 as indicated.

Table 1. Basic Safeguarding Requirements

BASIC SAFEGUARDING REQUIREMENT	NIST SP 800-171 REQUIREMENT
Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems)	3.1.1
Limit information system access to the types of transactions and functions that authorized users are permitted to execute	3.1.2
Verify and control/limit connections to, and use of, external information systems	3.1.20
Control information posted or processed on publicly accessible information systems	3.1.22
Identify information system users, processes acting on behalf of users, or devices	3.5.1
Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems	3.5.2
Sanitize or destroy information system media containing nonpublic DoD information before disposal or release for reuse	3.8.3
Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals	3.10.1
Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices	3.10.3, 3.10.4, and 3.10.5
Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems	3.13.1
Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks	3.13.5
Identify, report, and correct information and information system flaws in a timely manner	3.14.1
Provide protection from malicious code at appropriate locations within organizational information systems	3.14.2
Update malicious code protection mechanisms when new releases are available	3.14.4
Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed	3.14.5

3.3. CYBER INCIDENT REPORTING AND RESPONSE. In accordance with DoD's DIB Cyber Security Activities Federal Rule, Part 236 of Title 32, Code of Federal Regulations, DoD Components must, through relevant contracts or other agreements, require non-DoD entities to report and respond to cyber incidents affecting their information systems that process, store, or

transmit DoD CUI as specified in the following subparagraphs. This is typically implemented contractually in accordance with DFARS 252.204-7012.

a. Cyber Incident Reporting Requirement.

(1) When a non-DoD entity discovers a cyber incident, the non-DoD entity must conduct a review for evidence of compromise of DoD CUI. The review should include analyzing the non-DoD entity's information system(s) that were part of the cyber incident, including, but not limited to, identifying compromised computers, servers, specific data, user accounts, and other information systems on the non-DoD entity's network(s) that may have been accessed as a result of the cyber incident, in order to identify compromised DoD CUI and report cyber incidents to DoD.

(2) The non-DoD entity will rapidly report (within 72-hours of discovery) all cyber incidents affecting DoD CUI on unclassified information systems through the web portal at https://dibnet.dod.mil. Upon receipt, DC3 will provide a copy of the report to the appropriate contracting officer or designated government representative.

b. Medium Assurance Certificate Requirement. The non-DoD entity must have or acquire a DoD-approved medium assurance certificate to report cyber incidents. Information on obtaining a DoD-approved medium assurance public key infrastructure certificate can be found on the External Certification Authority Program Website at https://iase.disa.mil/pki/eca/Pages/index.aspx

c. Malicious Software Requirement. When the non-DoD entity discovers and isolates malicious software (also referred to as malicious code) in connection with a reported cyber incident, the non-DoD entity must submit the malicious software to the DC3 in accordance with instructions provided by DC3 or the contracting officer.

d. Media Preservation and Protection Requirement. When a non-DoD entity discovers a cyber incident has occurred, the non-DoD entity must preserve and protect images of all known affected information systems and all relevant monitoring and packet capture data for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest through DoD processes established by the USD(R&E).

e. Access for Forensic Analysis Requirement. Upon request from a DoD Component, the non-DoD entity must provide DoD access to additional information or equipment that is necessary to conduct a forensic analysis.

f. Cyber Incident Damage Assessment Requirement. If the DoD Component elects to conduct a damage assessment, the DoD Component will, following processes established by the USD(R&E), request that the non-DoD entity provide all of the damage assessment information gathered in accordance with Paragraph 3.3.d.

g. DoD Safeguarding and Use of Non-DoD Entity Attributional or Proprietary Information. DoD Components will protect against unauthorized use or release of information obtained from the non-DoD entity (or derived from information obtained from the non-DoD

entity) that contains non-DoD entity attributional or proprietary information, including such information submitted in accordance with Paragraph 3.3.a.

3.4. VALIDATION AND COMPLIANCE.

a. When warranted based on the criticality of the information provided to, or developed by, the non-DoD entity, DoD Components will include a requirement in the solicitation for the non-DoD entity to describe implementation of the requirements of NIST SP 800-171, and as appropriate, include a requirement for the non-DoD entity to demonstrate compliance before or upon award of the contract, grant, or execution of another legal agreement. The DoD Component may include a requirement in the solicitation for the non-DoD entity to notify the DoD Component when there is a deficiency that affects DoD information, or to periodically review how they are resolving deficiencies and meeting requirements, or both. Additionally, for contracts that include the clause at DFARS 252.204-7012, the DoD Component's contracting officer may request the contractor for an assessment of the contractor's compliance with the requirements of that clause upon receipt of a cyber incident report.

b. DoD Components should not intrude into the operations, maintenance, or governance of the non-DoD entity's internal information system by specifying the content and format of plans of action that address deficiencies, or specifying the parameters of security controls.

GLOSSARY

G.1. ACRONYMS.

CIO	chief information officer
CNSSI	Committee on National Security Systems instruction
CUI	controlled unclassified information
DC3	DoD Cyber Crime Center
DFARS	Defense Federal Acquisition Regulation Supplement
DIB	Defense Industrial Base
DoDD	DoD directive
DoDI	DoD instruction
FAR	Federal Acquisition Regulation
NIST SP	National Institute of Standards and Technology Special Publication
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment
USD(I)	Under Secretary of Defense for Intelligence
USD(R&E)	Under Secretary of Defense for Research and Engineering

G.2. DEFINITIONS. Unless otherwise noted, these terms and their definitions are for the purpose of this issuance.

adequate security. Defined in Committee on National Security Systems Instruction (CNSSI) 4009.

compromise. Defined in CNSSI 4009.

non-DoD entity attributional/proprietary information. Information that identifies the contractor(s), whether directly or indirectly, by the grouping of information that can be traced back to the contractor(s) (e.g., program description, facility locations), personally identifiable information, as well as trade secrets, commercial or financial information, or other commercially sensitive information that is not customarily shared outside of the company.

CUI. Defined in Volume 4 of DoD Manual 5200.01.

controlled technical information. Technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in

DoDI 5230.24. The term does not include information that is lawfully publicly available without restrictions.

cyber incident. Actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

DoD CUI. CUI that is marked or otherwise identified and provided to a non-DoD entity by or on behalf of DoD in support of the performance of a contract, grant or other legal agreement; or collected, developed, received, transmitted, used, or stored by or on behalf of the non-DoD entity in support of the performance of the contract, grant or other legal agreement.

DoD information. Any information that is in DoD custody and control; relates to information in DoD custody and control; was acquired by DoD employees as part of their official duties or because of their official status within DoD, including information that is provided by the DoD to a non-DoD entity; or is developed by a non-DoD entity in support of an official DoD activity.

DIB. Defined in the DoD Dictionary of Military and Associated Terms.

federal contract information. Defined in FAR 52.204-21. An example of nonpublic DoD information when it relates to a DoD contract.

IT service. Defined in DoDI 8500.01.

malicious code. Defined in CNSSI 4009.

malicious software. Computer software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. This definition includes a virus, worm, Trojan horse, or other code-based entity that infects a host, as well as spyware and some forms of adware.

media. Defined in CNSSI 4009.

mission partner. Defined in DoDD 8000.01.

non-DoD entity. Any person who is not a civilian employee or military member of the DoD, or any entity or organization that is not a DoD Component. This includes any non-DoD federal agency and its personnel, and any contractor, grantee, awardee, partner, or party to any form of legal agreement with the DoD or another federal agency.

non-DoD information system. Any information system that is not owned, controlled, or operated by the DoD and that is not used or operated by a contractor or other non-DoD entity exclusively on behalf of the DoD. Includes information systems owned and operated by other departments and agencies of the U.S. Government; State and local governments; allies, coalition members, host nations and other nations; multinational organizations; non-governmental organizations; and the private sector.

nonpublic DoD information. Any DoD information that has not been cleared for public release in accordance with DoDD 5230.09. Nonpublic DoD information includes federal contract information that relates to a DoD contract.

on-behalf of. A situation that occurs when a non-executive branch entity uses or operates an information system or maintains or collects information for the purpose of processing, storing, or transmitting federal information; and those activities are not incidental to providing a service or product to the government.

public DoD information. DoD information that has been cleared for public release in accordance with DoDD 5230.09.

publicly available computer. Any computer available to the general public, usually after certain conditions are met (e.g., payment of a fee, a paying guest in a hotel).

REFERENCES

Code of Federal Regulations, Title 32

Committee on National Security Systems Instruction No. 4009, "Committee on National Security Systems (CNSS) Glossary," April 6, 2015

Defense Federal Acquisition Regulation Supplement 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting," current edition

DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," November 21, 2014, as amended

DoD Directive 5230.09, "Clearance of DoD Information for Public Release," August 22, 2015

DoD Directive 5505.13E, "DoD Executive Agent (EA) for the DoD Cyber Crime Center (DC3)," March 1, 2010, as amended

DoD Directive 8000.01, "Management of the Department of Defense Information Enterprise (DoD IE)," March 17, 2016, as amended

DoD Instruction 4000.19, "Support Agreements," April 25, 2013, as amended

DoD Instruction 5205.13, "Defense Industrial Base (DIB) Cyber Security (CS) Activities," January 29, 2010, as amended

DoD Instruction 5230.24, "Distribution Statements on Technical Documents," August 23, 2012, as amended

DoD Instruction 8500.01, "Cybersecurity," March 14, 2014

DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 13, 2014, as amended

DoD Manual 5200.01, Volume 4, "DoD Information Security Program: Controlled Unclassified Information (CUI)," February 24, 2012

Federal Acquisition Regulation 52.204-21, "Basic Safeguarding of Covered Contractor Information Systems," current edition

Federal Information Processing Standards Publication 199, "Standards for Security Categorization of Federal Information and Information Systems," February 2004

National Institute of Standards and Technology Special Publication 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," December 2016, as amended

Office of the Chairman of the Joint Chiefs of Staff, "DoD Dictionary of Military and Associated Terms," current edition