Controlled Unclassified Information (CUI)

GLOSSARY and POLICY SUMMARIES

Version 2.0

INSIDE ...

GLOSSARY

Agency is any executive agency as defined in 5 U.S.C. 105; the United States Postal Service; and any other independent entity within the executive branch that designates or handles CUI.

Agency CUI policies are the policies the agency enacts to implement the CUI program within the specific agency. They must be consistent with EO 13556, 32 CFR Part 2002, and the CUI Registry and coordinated with the CUI Executive Agent (EA).

Agreements and Arrangements are any vehicle that sets out specific CUI handling requirements for contractors and other information-sharing partners when the arrangement with the other party involves CUI. Agreements and arrangements include, but are not limited to, contracts, grants, licenses, certificates, memorandum of agreements/ arrangements or understandings, and information-sharing agreements or arrangements. When disseminating or sharing CUI with non-executive branch entities, agencies should enter into written agreements or arrangements that include CUI provisions whenever feasible (see 32 CFR 2002.16(a)(5) and 32 CFR 2002.16(a)(6) for details). When sharing information with foreign entities, agencies should enter agreements or arrangements when feasible (see 32 CFR 2002.16(a)(5)(iii) and 32 CFR 2002.16(a)(6) for details).

Authorized holder is an individual, agency, organization, or group of users that is permitted to designate or handle CUI, in accordance with 32 CFR Part 2002.

Classified National Security Information is information that has been determined pursuant to EO 13526, or any predecessor order, to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

Controlled Environment is any area or space an authorized holder deems to have adequate physical or procedural controls (e.g., barriers or managed access controls) to protect CUI from unauthorized access or disclosure.

Controlled Unclassified Information (CUI) is information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. However, CUI does not include classified information (see definition above) or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency. Law, regulation, or Government-wide policy may require or permit safeguarding or dissemination controls in three ways: Requiring or permitting agencies to control or protect the information but providing no specific controls, which makes the information CUI Basic; requiring or permitting agencies to control or protect the information and providing specific controls for doing so, which makes the information CUI Specified; or requiring or permitting agencies to control the information and specifying only some of those controls, which makes the information CUI Specified, but with CUI Basic controls where the authority does not specify.

Controls are safeguarding or dissemination controls that a law, regulation, or Government-wide policy requires or permits agencies to use when handling CUI. The authority may specify the controls it requires or permits the agency to apply, or the authority may generally require or permit agencies to control the information (in which case, the agency applies the controls from Executive Order 13556, 32 CFR Part 2002, and the CUI Registry).

CUI Basic is the subset of CUI for which the authorizing law, regulation, or Government-wide policy does not set out specific handling or dissemination controls. Agencies handle CUI Basic according to the uniform set of controls set forth in this part and the CUI Registry. CUI Basic differs from CUI Specified (see definition for CUI Specified), and CUI Basic controls apply whenever CUI Specified ones do not cover the involved CUI.

CUI categories and subcategories are those types of information for which laws, regulations, or Government-wide policies require or permit agencies to exercise safeguarding or dissemination controls, and which the CUI Executive Agent has approved and listed in the CUI Registry. The controls for any CUI Basic categories and any CUI Basic subcategories are the same, but the controls for CUI Specified categories and subcategories can differ from CUI Basic ones and from each other. A CUI category may be Specified, while some or all of its subcategories may not be, and vice versa. If dealing with CUI that falls into a CUI Specified category or subcategory, review the controls for that category or subcategory on the CUI Registry. Also consult the agency's CUI policy for specific direction from the Senior Agency Official.

CUI category or subcategory markings are the markings approved by the CUI Executive Agent for the categories and subcategories listed in the CUI Registry.

CUI Executive Agent (EA) is the National Archives and Records Administration (NARA), which implements the executive branch-wide CUI Program and oversees Federal agency actions to comply with Executive Order 13556. NARA has delegated this authority to the Director of the Information Security Oversight Office (ISOO).

CUI Program is the executive branch-wide program to standardize CUI handling by all Federal agencies. The Program includes the rules, organization, and procedures for CUI, established by Executive Order 13556 and 32 CFR Part 2002.

CUI Program Manager is an agency official, designated by the agency head or CUI Senior Agency Official, to serve as the official representative to the CUI Executive Agent on the agency's day-to-day CUI Program operations, both within the agency and in interagency contexts.

CUI Registry is the online repository for all information, guidance, policy, and requirements on handling CUI, including everything issued by the CUI Executive Agent other than 32 CFR Part 2002. Among other information, the CUI Registry identifies all approved CUI categories and subcategories, provides general descriptions for each, identifies the basis for controls, establishes markings, and includes guidance on handling procedures.

CUI Senior Agency Official (SAO) is a senior official designated in writing by an agency head and responsible to that agency head for implementation of the CUI Program within that agency. The CUI Senior Agency Official is the primary point of contact for official correspondence, accountability reporting, and other matters of record between the agency and the CUI Executive Agent.

CUI Specified is the subset of CUI in which the authorizing law, regulation, or Government-wide policy contains specific handling controls that it requires or permits agencies to use that differ from those for CUI Basic. The CUI Registry indicates which laws, regulations, and Government-wide policies include such specific requirements. CUI Specified controls may be more stringent than, or may simply differ from, those required by CUI Basic; the distinction is that the underlying authority spells out the controls for CUI Specified information and does not for CUI Basic information. CUI Basic controls apply to those aspects of CUI Specified where the authorizing laws, regulations, and Government-wide policies do not provide specific guidance.

Decontrolling occurs when an authorized holder, consistent with 32 CFR Part 2002 and the CUI Registry, removes safeguarding or dissemination controls from CUI that no longer requires such controls. Decontrol may occur automatically or through agency action. See 32 CFR 2002.18.

Designating CUI occurs when an authorized holder, consistent with 32 CFR Part 2002 and the CUI Registry, determines that a specific item of information falls into a CUI category or subcategory. The authorized holder who designates the CUI must make recipients aware of the information's CUI status in accordance with 32 CFR Part 2002.

Designating agency is the executive branch agency that designates or approves the designation of a specific item of information as CUI.

Disseminating occurs when authorized holders provide access, transmit, or transfer CUI to other authorized holders through any means, whether internal or external to the agency.

Document means any tangible thing which constitutes or contains information, and means the original and any copies (whether different from the originals because of notes made on such copies or otherwise) of all writings of every kind and description over which an agency has authority, whether inscribed by hand or by mechanical, facsimile, electronic, magnetic, microfilm, photographic, or other means, as well as phonic or visual reproductions or oral statements, conversations, or events, and including, but not limited to: Correspondence, email, notes, reports, papers, files, manuals, books, pamphlets, periodicals, letters, memoranda, notations, messages, telegrams, cables, facsimiles, records, studies, working papers, accounting papers, contracts, licenses, certificates, grants, agreements, computer disks, computer tapes, telephone logs, computer mail, computer printouts, worksheets, sent or received communications of any kind, teletype messages, agreements, diary entries, calendars and journals, printouts, drafts, tables, compilations, tabulations, recommendations, accounts, work papers, summaries, address books, other records and recordings or transcriptions of conferences, meetings, visits, interviews, discussions, or telephone conversations, charts, graphs, indexes, tapes, minutes, contracts, leases, invoices, records of purchase or sale correspondence, electronic or other transcription of taping of personal conversations or conferences, and any written, printed, typed, punched, taped, filmed, or graphic matter however produced or reproduced. Document also includes the file, folder, exhibits, and containers, the labels on them, and any metadata, associated with each original or copy. Document also includes voice records, film, tapes, video tapes, email, personal computer files, electronic matter, and other data compilations from which information can be obtained, including materials used in data processing.

Federal Information System is an information system used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency (44 U.S.C. 3554(a)(1)(A)(ii)).

Foreign Entity is a foreign government, an international organization of governments or any element thereof, an international or foreign public or judicial body, or an international or foreign private or non-governmental organization.

Formerly Restricted Data (FRD) is a type of information classified under the Atomic Energy Act, and defined in 10 CFR 1045, Nuclear Classification and Declassification.

Handling is any use of CUI, including but not limited to marking, safeguarding, transporting, disseminating, re-using, and disposing of the information.

Lawful Government Purpose is any activity, mission, function, operation, or endeavor that the U.S. Government authorizes or recognizes within the scope of its legal authorities or the legal authorities of non-executive branch entities (such as state and local law enforcement).

Legacy Material is unclassified information that an agency marked as restricted from access or dissemination in some way, or otherwise controlled, prior to the CUI Program.

Limited Dissemination Control is any CUI Executive Agent-approved control that agencies may use to limit or specify CUI dissemination.

Misuse of CUI occurs when someone uses CUI in a manner not in accordance with the policy contained in Executive Order 13556, 32 CFR Part 2002, the CUI Registry, agency CUI policy, or the applicable laws, regulations, and Government-wide policies that govern the affected information. This may include intentional violations or unintentional errors in safeguarding or disseminating CUI. This may also include designating or marking information as CUI when it does not qualify as CUI.

National Security System is a special type of information system (including telecommunications systems) whose function, operation, or use is defined in National Security Directive 42 and 44 U.S.C. 3542(b)(2).

Non-executive branch entity is a person or organization established, operated, and controlled by individual(s) acting outside the scope of any official capacity as officers, employees, or agents of the executive branch of the Federal Government. Such entities may include: Elements of the legislative or judicial branches of the Federal Government; state, interstate, tribal, or local government elements; and private organizations. Non-executive branch entity does not include foreign entities as defined in 32 CFR Part 2002, nor does it include individuals or organizations when they receive CUI information pursuant to federal disclosure laws, including the Freedom of Information Act (FOIA) and the Privacy Act of 1974.

On behalf of an agency 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.

Order is Executive Order 13556, Controlled Unclassified Information, November 4, 2010 (3 CFR, 2011 Comp., p. 267), or any successor order.

Portion is ordinarily a section within a document, and may include subjects, titles, graphics, tables, charts, bullet statements, sub-paragraphs, bullets points, or other sections.

Protection includes all controls an agency applies or must apply when handling information that qualifies as CUI.

Public Release occurs when the agency that originally designated particular information as CUI makes that information available to the public through the agency's official public release processes. Disseminating CUI to non-executive branch entities as authorized does not constitute public release. Releasing information to an individual pursuant to the Privacy Act of 1974 or disclosing it in response to a FOIA request also does not automatically constitute public release, although it may if that agency ties such actions to its official public release processes. Even though there may be circumstances in which an agency may be required to disclose CUI to a member of the public, the Government must still control the CUI it holds unless it publicly releases it through its official public release processes.

Records are agency records and Presidential papers or Presidential records (or Vice-Presidential), as those terms are defined in 44 U.S.C. 3301 and 44 U.S.C. 2201 and 2207. Records also include such items created or maintained by a Government contractor, licensee, certificate holder, or grantee that are subject to the sponsoring agency's control under the terms of the entity's agreement with the agency.

Required or permitted (by a law, regulation, or Government-wide policy) is the basis by which information may qualify as CUI. If a law, regulation, or Government-wide policy requires that agencies exercise safeguarding or dissemination controls over certain information, or specifically permits agencies the discretion to do so, then that information qualifies as CUI. The term 'specifically permits' in this context can include language such as 'is exempt from' applying certain information release or disclosure requirements, "may" release or disclose the information, "may not be required to" release or disclose the information, "is responsible for protecting" the information, and similar specific but indirect, forms of granting the agency discretion regarding safeguarding or dissemination controls. This does not include general agency or agency head authority and discretion to make decisions, risk assessments, or other broad agency authorities, discretions, and powers, regardless of the source. The CUI Registry reflects all appropriate authorizing authorities.

Restricted Data (RD) is a type of information classified under the Atomic Energy Act, defined in 10 CFR 1045, Nuclear Classification and Declassification.

Re-use means incorporating, restating, or paraphrasing CUI from its originally designated form into a newly created document.

Self-inspection is an agency's internally managed review and evaluation of its activities to implement the CUI Program.

Unauthorized Disclosure (UD) occurs when an authorized holder of CUI intentionally or unintentionally discloses CUI without a lawful Government purpose, in violation of restrictions imposed by safeguarding or dissemination controls, or contrary to limited dissemination controls.

Uncontrolled Unclassified Information is information that neither Executive Order 13556 nor classified information authorities cover as protected. Although this information is not controlled or classified, agencies must still handle it in accordance with Federal Information Security Modernization Act (FISMA) requirements.

Working Papers are documents or materials, regardless of form, that an agency or user expects to revise prior to creating a finished product.

ACRONYMS

CDSE	Center for Development of Security Excellence
CFR	Code of Federal Regulations
CMMC	Cybersecurity Maturity Model Certification
CNSI	Classified National Security Information
CMT	Classification Marking Tools
COA	Course of Action
CSA	Cognizant Security Agency
CSSO	Contractor Special Security Officer
CUI	Controlled Unclassified Information
DCSA	Defense Counterintelligence and Security Agency
DFARS	Defense Federal Acquisition Regulation Supplement
DIA	Defense Intelligence Agency
DISS	Defense Information System for Security
DODI	DOD Instruction
DOS	Department of State
DTA	Data Transfer Agent
ESO	Enterprise Security Operations
FAQ	Frequently Asked Questions
FCI	Federal Contract Information
FCL	Facility Security Clearance
FedRamp	Federal Risk and Authorization Management Program
FOUO	For Official Use Only
FSO	Facility Security Officer
GCA	Government Contracting Activity
GCC	Government Cloud Computing
HIPPA	Health Insurance Portability and Accountability Act
IO	Information Owner
ISL	Industrial Security Letter
ISOO	Information Security Oversight Office
ISWG	Industrial Security Working Group
ITAR	International Traffic in Arms Regulations
LDC	Limited Dissemination Control
NARA	National Archives and Records Administration
NCAISS	National Central Access Information Security System
NISPOM	National Industrial Security Program Operating Manual
NISS	National Industrial Security System
NISP	National Industrial Security Program
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OCA	Original Classification Authority
PII	Personally Identifiable Information
POAM	Plan of Action and Milestones
POC	Point of Contact
SBU	Sensitive but Unclassified
SCG	Security Classification Guide
SF	Standard Form
SPP	Standard Practice Procedure
SPRS	Supplier Performance Risk System
TTB	Alcohol and Tobacco Tax and Trade Bureau
USD(I&S)	Under Secretary of Defense for Intelligence and Security
USG	United States Government

32 CFR Part 2002 – Controlled Unclassified Information (CUI)

Policy Date: September 14, 2016

Complete Policy: 32 CFR Part 2002

Stakeholders Impacted:

- All executive branch agencies that designate or handle CUI.
- Any contractors or information-sharing partners that receive CUI through incorporations into agreements.

Policy Overview:

- Defines CUI.
- Describes the CUI Program and establishes policy for designating, handling, and decontrolling CUI.
- Outlines the roles and responsibilities of the CUI Executive Agent (EA), Agency Heads, and the CUI SAO (Senior Agency Official).
- Describes NARA's delegation of EA responsibilities to ISOO.
- Includes guidance on the CUI Registry, CUI categories and subcategories, safeguarding, accessing and disseminating, decontrolling, marking, limitations on applicability of agency CUI policies, agency and self-inspection programs for CUI.
- Contains guidance on education and training, CUI cover sheets, transferring records, legacy materials, waivers of CUI requirements, CUI and disclosure statutes, CUI and the Privacy Act, CUI and the Administrative Procedure Act (APA), challenges to CUI designations, dispute resolution for agencies, and misuse of CUI.

Policy Highlights:

CUI Registry:

- Requires the CUI EA to maintain the CUI Registry which is the authoritative central repository for the CUI Program.

CUI Categories and Subcategories:

- Explains the purpose of CUI categories and sub-categories for identifying unclassified information that requires or permits agencies to handle by means of safeguarding or dissemination controls.

Safeguarding:

- Requires Authorized holders to safeguard CUI using CUI Basic or CUI Specified.
- Authorizes holders to destroy CUI when the agency no longer needs the information, requiring them to render it unreadable, indecipherable, and irrecoverable.

Accessing and Disseminating:

- Provides guidance for accessing and disseminating CUI if it meets the following:
  1. Abides by the laws, regulations, or Government-wide policies.
  2. Furthers a lawful Government purpose.
  3. Is not restricted by an authorized limited dissemination control.
  4. Is not otherwise prohibited by law.

Decontrolling:

- Sets expectations for agencies to decontrol any CUI designated by their agency that no longer requires safeguarding or dissemination controls, unless doing so conflicts with the governing law, regulation, or government-wide policy.

Self-inspection programs:

- Requires agencies to create a self-inspection program.

Training:

- Requires agencies to establish a training policy and train employees at least once every two years.

POLICY SUMMARIES

DODI 5200.48

Policy Date: March 6, 2020

Complete Policy: DODI 5200.48, “Controlled Unclassified Information (CUI)"

Stakeholders Impacted:

- 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 DOD Components.
- Applies to Industry when incorporated into and levied via arrangements, agreements, contracts, and other actions requiring access to CUI.

Policy Overview:

- Includes the responsibilities of USD (I&S), Director for Defense Intelligence (Counterintelligence, Law Enforcement, and Security (DDI(CL&S)), Director, Defense Counterintelligence and Security Agency (DCSA) Chief Management Officer of the Department of Defense (CMO), PFPA, Under Secretary of Defense for Policy, USD Acquisition and Sustainment (A&S), USD Research and Engineering (R&E), DOD Chief Information Officer (CIO), OSD and DOD Component Heads, Secretaries of the Military Departments, and the Chairman of the Joint Chiefs of Staff.
- Includes background on the program, legacy information requirements, handling requirements, marking requirements, general DOD CUI administrative requirements, DOD CUI procedures, DOD CUI requirements, Original Classification Authorities (OCAs,) release and disclosure requirements, and system and network CUI requirements.
- Covers dissemination and includes application of CUI to DOD industry.

Policy Highlights:

Legacy Information Requirements:

- Does not require DOD legacy material to be re-marked or redacted while it remains under DOD control. Requires any such document or new derivative document to be marked as CUI if shared outside of DOD.
- Requires DOD legacy information to be reviewed by the owner to determine if it meets CUI requirements.

Marking Requirements:

- Requires “CUI” in the banner and footer of unclassified DOD documents.
- If portion marking, requires all document subjects, titles, individual sections, parts, paragraphs, or other portions of a CUI document known to contain CUI, to be marked with “(CUI)”. Requires “(CUI)” portion markings in classified documents.

DOD CUI Procedures:

- Requires the authorized holder of a document or material to determine whether information falls into a CUI category.
- Includes 11 training standard requirements.

Dissemination, Decontrolling, and Destruction of CUI:

- Requires dissemination controls to deem the audience to have a lawful government purpose to use the CUI and specify the rationale for applying the controls.
- Requires agencies to promptly decontrol CUI determined by the owner to no longer require safeguarding or dissemination controls.
- Relieves authorized holders from handling requirements when CUI is decontrolled.
- Constitutes the decontrol of a document if the authorized holder of the CUI publicly releases it in accordance with authorized procedures.

Application to Industry:

- Identifies NIST SP 800-171 as the baseline CUI system security requirements for industry.
- Requires enhanced protection for CUI with the potential to impact national security.
- Requires non-DOD Information System (IS) processing, storing, or transmitting of CUI to be safeguarded in accordance with contractual requirements.
- Requires compliance with safeguarding requirements identified in the contract for all types of CUI for contractors, sub-contractors, and consultants.
- Requires the program office or requiring activity to identify DOD CUI at the time of contract award, provide guidance on information aggregation or compilation, and to review recurring or renewed contracts for CUI to comply with this issuance.

DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting

Policy Date: January 2023 (Change Effective)

Complete Policy: DFARS (acquisition.gov)

Stakeholders Impacted:

- This clause is required in all DoD contracts and subcontracts for which performance will involve covered defense information or operationally critical support.

Policy Overview:

- The clause requires that contractors implement minimum information security protections to provide adequate security on all covered contractor information, cyber incident reporting, isolating and submitting malicious software, preserving and protecting media images of all known affected information systems, provide DOD with access to additional information or equipment necessary for forensic analysis, cyber incident damage assessment activities, DOD safeguarding and use of contractor attributional/proprietary information, use and release of contractor attributional/proprietary information not created by or for DOD, and other safeguarding or reporting requirements.

Policy Highlights:

Safeguarding covered defense information:

- Contractors and subcontractors must implement NIST SP 800-171 as soon as practical in order to effectively safeguard covered defense information.

Reporting cyber incidents:

- Contractors are required to report incidents that affect covered defense information or the contractor's ability to perform requirements designated as operationally critical support. The contractor shall conduct a review for evidence of compromise and rapidly report cyber incidents to DOD.

Submitting malicious software:

- If discovered and isolated in connection with a reported cyber incident, the contractor or subcontractor must submit the malicious software to the DOD Cyber Crime Center.

Facilitating damage assessment:

- If the DOD elects to conduct a damage assessment, the Contracting Officer will be notified by the requiring activity to request media and damage assessment information from the contractor.

Corresponding CUI DFARS Clauses:

- DFARS 252.204-7019 Notice of NIST SP 800-171 DoD Assessment Requirements
- DFARS 252.204-7020 NIST SP 800-171 DoD Assessment Requirements
- DFARS 252.204-7021 Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirement
- DFARS 252.204-7024 Notice on the Use of the Supplier Performance Risk Performance System

FOR MORE INFORMATION:
Contact Your Local Industrial Security Representative or
the DCSA Enterprise Security Operations CUI Mailbox at:
dcsa.quantico.ctp.mbx.eso-cui@mail.mil