CONTROLLED
UNCLASSIFIED
INFORMATION

CUI SELF-INSPECTION TOOL
FOR DOD & INDUSTRY

CUI SELF-INSPECTION TOOL
FOR DOD & INDUSTRY

This Controlled Unclassified Information (CUI) Self-Inspection Tool is a resource intended to provide both the Department of Defense (DOD) and Industry the ability to review and evaluate CUI programs to determine their compliance and effectiveness.

The tool highlights requirements for a standard DOD CUI Program contained in the DOD Instruction 5200.48, based on Executive Order (EO) 13556, 32 Code of Federal Regulations (CFR) Part 2002, National Institute of Standards and Technology (NIST) 800-171, and Defense Counterintelligence and Security Agency (DCSA) guidance.

The following elements assist DOD and Industry in establishing a CUI program, identifying gaps and vulnerabilities, and achieving compliance. The tool is meant to serve as an overarching guide addressing the various types of elements under each area of a CUI program.

ELEMENTS OF A CUI OVERSIGHT PROGRAM

1. CUI Program Management
2. CUI Identification & Registry
3. CUI Markings
4. CUI Sharing (Dissemination & Distribution)
5. CUI Safeguarding and Storage
6. CUI Decontrol
7. Telecommunications, Information Systems, and Network Security
8. Reproduction
9. Disposition and Destruction
10. Transmission and Transportation
11. Security Education and Training
12. Security Incidents and CUI Misuse to include Compromises

Not all of the elements/considerations within this tool will apply to each DOD Agency or Component, or Industry CUI program, and must be reviewed for applicability prior to adhering to compliance. In all cases, regulatory guidance should take priority over company established procedures.

1. CUI PROGRAM MANAGEMENT

The DODI 5200.48 is an initial implementation of all the requirements detailed in the 32 CFR Part 2002 regarding the components of a CUI oversight program. It includes the minimum requirements and partially addresses certain ones based on current capabilities across DOD. Additional processes and procedures for specific implementation will be covered in supporting DOD issuances. Until such time, DCSA is creating a series of CUI job aids and resources to provide more in-depth descriptions for the various implementation areas. All Government Contracting Activity (GCA) issued contracts must identify the requirements and terms under which a contractor may have access to, create, collect, utilize, process, store, maintain, disseminate, disclose, or dispose of CUI. For further comprehensive guidance on CUI Program Management, DCSA has created a "CUI Baseline Requirements" job aid and a "Roadmap to Compliance" job aid which can be found at https://www.dcsa.mil/mc/ctp/cui/.

Below are some considerations for establishing a CUI program. Ensure the CUI Manager implements the following as it relates to CUI Program Management:

Has the Agency or Component or Cleared Contractor:	**Yes**	**No**	**N/A**	**Notes**
Appointed a CUI Manager or other personnel to manage and implement the CUI Program which implements the provisions of DODI 5200.48? (32 CFR 2002.4.c, DODI 5200.48 (5.3))				
Developed and implemented security guidance necessary for program implementation. (32 CFR 2002.4.c, DODI 5200.48(5.3))				
Allocated sufficient resources and personnel committed to implement the CUI Program? (32 CFR 2002.4.c, DODI 5200.48 (5.3))				
Conduct CUI oversight review of their contracts that contain Government Contracting Office CUI oversight requirements. (32 CFR 2002.16.5, DODI 5200.48 (5.3))				
Established, implemented, and maintained an effective security education program as required by DODI 5200.48, to include initial mandatory and continuing/refresher training for assigned members. (32 CFR 2002.30, DODI 5200.48 (3.6)g)				
Industry Only: Does the contractor have DOD contracts with CUI requirements? (32 CFR 2002.16.5, DODI 5200.48 (5.3))				
Industry Only: Does the contractor have non-DOD contracts with CUI requirements? (32 CFR 2002.16.5 DODI 5200.48 (5.3))				
Has the CUI Manager completed mandatory CUI training? (32 CFR 2002.30, DODI 5200.48 (3.6)b)				
Have personnel working with CUI completed mandatory CUI training? (32 CFR 2002.30.b, DODI 5200.48 (3.6)b)				
Is the CUI Manager documenting CUI oversight training? If so, how is it tracked? (32 CFR 2002.30, DODI 5200.48 (3.6)b)				
Are procedures established to prevent unauthorized access to, and disclosure of CUI? (32 CFR 2002.14c 3, DODI 5200.48 (5.3))				
Are emergency procedures developed for the protection, removal, or destruction of CUI material in case of fire, natural disaster, civil disturbance, or terrorist activities to minimize the risk of compromise? (32 CFR 2002.14c 3, DODI 5200.48 (5.3))				

2. CUI IDENTIFICATION & REGISTRY

DOD Agencies, Components, and Industry should consult the CUI registry to become aware of CUI categories and organizational index groupings at https://www.archives.gov/cui and https://www.dodcui.mil/Home/DoD-CUI-Registry/.

Below are some considerations for establishing a CUI program. Ensure the CUI Manager implements the following as it relates to identifying CUI:

REVIEW ITEM	Yes	No	N/A	Notes
Are personnel who identify CUI categories trained on the process and requirements for applying the information in the CUI Registry? (32 CFR 2002.10, DODI 5200.48 (3.3))				
Do employees with access to CUI information know how to use the CUI Registry to identify Indexes for CUI category groups? (32 CFR 2002.10, DODI 5200.48 (3.6)f)				
Do employees with access to CUI information know how to identify individual CUI categories? (32 CFR 2002.10, DODI 5200.48 (3.6)f)				
Do employees with access to CUI information know how to use the DOD issuances to help identify a CUI category? (32 CFR 2002.10, DODI 5200.48 (3.6)f)				
Do employees with access to CUI information understand CUI prohibitions and limitations? (32 CFR 2002.10, DODI 5200.48 (3.3)d)				
Do employees with access to CUI information know CUI responsibilities for identification in DOD contracts? (32 CFR 2002.10, DODI 5200.48 (5.1))				
Do personnel use the available resources to help identify CUI, such as websites and authoritative publications? (32 CFR 2002.10, DODI 5200.48 (3.6)f)				
Do personnel know how to use the CUI Registry to identify indexes for CUI category groups? (32 CFR 2002.10, DODI 5200.48 (3.6)f)				

3. CUI MARKINGS

At a minimum, CUI markings for unclassified DOD documents will include the acronym "CUI" in the banner and footer of the document. Portion markings may also be used but are not required. For further comprehensive guidance on CUI marking DCSA has made available several marking job aids on its website at https://www.dcsa.mil/mc/ctp/cui/.

Below are some considerations for establishing a CUI program. Ensure the CUI Manager implements the following as it relates to CUI markings:

REVIEW ITEM	Yes	No	N/A	Notes
Are persons who apply CUI markings trained on the process and requirements to include on documents and materials? (32 CFR 2002.20, DODI 5200.48 (3.4))				
Does "CUI" appear in the banner and footer of CUI documents? (32 CFR 2002.20, DODI 5200.48 (3.4))				
Are employees correctly applying the application of the CUI Designation Indicator Block? (32 CFR 2002.20, DODI 5200.48 (3.4))				
Is there a process in place to ensure "U//CUI" is NOT being applied? (32 CFR 2002.20, DODI 5200.48 (3.4))				
Where appropriate, are cover sheets used, and is the SF 901(b) properly marked? (32 CFR 2002.20, DODI 5200.48 (3.4))				
If CUI labels are used (SF 902/903), are they correctly applied to materials? • Are all charts, graphs, photographs, illustrations, figures, and similar items within documents marked CUI? • Are all CUI markings placed correctly within charts, graphs, photographs, illustrations, figures, etc., or next to the item? (32 CFR 2002.20, DODI 5200.48 (3.4))				
Are all files, folders, and groups of documents clearly marked on the outside of the file or folder (attaching a CUI cover sheet to the front of the folder or holder will satisfy this requirement)? (32 CFR 2002.20, DODI 5200.48 (3.4))				
Are all removable storage media (e.g. magnetic tape reels, disk packs, diskettes, CD-ROMS, removable hard disks, disk cartridges, tape cassettes, etc.) marked with the appropriate Standard Form label, if used? (32 CFR 2002.20, DODI 5200.48 (3.4))				

4. CUI SHARING (DISSEMINATION & DISTRIBUTION)

Similar to other information requiring safeguarding, there are rules regarding dissemination and distribution of CUI. While the points below highlight this requirement, one should consult DODI 5200.48 for a more comprehensive description. Authorized holders may disseminate CUI in accordance with distribution statements and applicable laws. Dissemination is allowed as long as it complies with law, regulation, or Government-wide policy; furthers a lawful government purpose; is not restricted by Limited Dissemination Control (LDC); and is not otherwise prohibited by any other law, regulation, or Government-wide policy. CUI information and material can be sent via first class mail, parcel post, or bulk shipments. CUI can also be transmitted by e-mail when practical, via approved secure communications systems, or systems using other protective measures.

Below are some considerations for establishing a CUI program. Ensure the CUI Manager implements the following as it relates to dissemination and distribution of CUI:

REVIEW ITEM	Yes	No	N/A	Notes
Are documents properly marked for limited dissemination control? (32 CFR 2002.16.3, DODI 5200.48 (4.2))				
Are documents properly marked for distribution when identified as containing Controlled Technical Information (CTI), export controlled, or scientific, technical, or engineering information? (32 CFR 2002.16.3, DODI 5200.48 (4.3))				
If the document requires a distribution statement, is the warning statement on the document? (32 CFR 2002.16.3, DODI 5200.48 (3.7))				
Is there a process in place to ensure the receiver of CUI has an authorized, lawful government purpose? (32 CFR 2002.16.3, DODI 5200.48 (4.2))				
Are there procedures in place to monitor CUI if it is to be shared with foreign partners? (32 CFR 2002.16.3, DODI 5200.48 (4.3))				
Are there procedures in place to monitor CUI if it is to be shared with non-DOD partners? (32 CFR 2002.16.3, DODI 5200.48 (4.2))				

5. CUI SAFEGUARDING AND STORAGE

In accordance with DODI 5200.48 and 32 CFR Part 2002, access to CUI is based on an authorized, lawful government purpose. DOD added "authorized" to provide a further trait to enhance safeguarding of CUI. This allows the owner of the CUI to determine if the individual or organization should be allowed access. It provides another layer of protection and awareness to the CUI owner who is accessing the information. For further comprehensive guidance on CUI program management, DCSA has created a "CUI Baseline Requirements" job aid and a "Roadmap to Compliance" job aid which can be found at https://www.dcsa.mil/mc/ctp/cui/.

Below are some considerations for establishing a CUI program. Ensure the CUI Manager implements the following as it relates to CUI safeguarding and storage:

REVIEW ITEM	Yes	No	N/A	Notes
Is there a program designed and maintained to optimize safeguarding of CUI? (32 CFR 2002.14, DODI 5200.48 (3.7))				
Are there control measures in place to prevent unauthorized access to CUI? (32 CFR 2002.14, DODI 5200.48 (3.7))				
Are personnel aware of procedures for identifying, reporting, and processing unauthorized disclosures of CUI? (32 CFR 2002. 14, DODI 5200.48 (3.6)g)				
Are there methods for transmitting CUI, preparing it correctly for mailing, and for hand carrying CUI materials? (32 CFR 2002.14)				
If CUI is removed from storage or the work environment, is it kept under constant surveillance of authorized persons? (32 CFR 2002.14)				
Are cover sheets or other measures offering one layer of protection placed on all documents if removed from storage or the work environment? (32 CFR 2002.32, DODI 5200.48 (3.4)f)				
Are equipment (e.g. copiers, facsimile machines, AIS equipment and peripherals, electronic typewriters and word processing systems) used for processing CUI protected from unauthorized access? (32 CFR 2002.14, DODI 5200.48 (5.1))				
Are only appropriately cleared and technically knowledgeable personnel allowed to inspect the equipment and media used for processing CUI before the equipment is removed from the protected areas? (32 CFR 2002.14, DODI 5200.48 (5.1))				

6. CUI DECONTROLLING

Similar to other information requiring safeguarding, there are rules regarding the decontrolling of CUI. While the points below highlight this requirement, one should consult DODI 5200.48 for a more comprehensive description. Once information is no longer CUI, it must be promptly decontrolled. Prior to decontrolling, the Director of the Washington Headquarters Services (WHS) will review CUI documents and materials for public release, in accordance with DODI 5230.09. Once it is determined that the information no longer requires protection from public disclosure, the Federal Government will notify all known holders of the decontrolled information.

Below are some considerations for establishing a CUI program. Ensure the CUI Manager implements the following as it relates to decontrolling of CUI:

REVIEW ITEM	Yes	No	N/A	Notes
Is there a records management system to facilitate public release of decontrolled documents? (32 CFR 2002.18.a, DODI 5200.48 (4.4))				
Is decontrolling of CUI performed by the authorized holder/originator or the designee? (32 CFR 2002.18.a, DODI 5200.48 (4.4))				
Are there procedures established for review of decontrolled CUI before public release? (32 CFR 2002.18.a, DODI 5200.48 (4.4))				

7. TELECOMMUNICATIONS, INFORMATION SYSTEMS, AND NETWORK SECURITY

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. CUI Managers are encouraged to work closely with those responsible for system security within their organization.

Below are some initial considerations for establishing a CUI program. Ensure the CUI Manager implements the following as it relates to Telecommunications, Information Systems, and Network Security:

REVIEW ITEM	Yes	No	N/A	Notes
Consistent with section 4.1(f) of E.O. 13556, 32 CFR Part 2002, and DODI 5200.48, and uniform procedures have been established to ensure automated information systems collecting, creating, communicating, computing, disseminating, processing, transmitting, or storing CUI are protected in accordance with applicable DOD policy issuances. (32 CFR 2002.16 g, DODI 5200.48, (3.10) NIST SP 800-171 2.2)				
Have procedures been established and implemented to:				
• Prevent access by unauthorized persons • Ensure the integrity of the information (32 CFR 2002.16 g, DODI 5200.48 (3.10), NIST SP 800-171 3.1.1)				
Has the facility created common information technology standards, protocols, and interfaces to maximize the availability of and access to the information in a form and manner facilitating its authorized use? (32 CFR 2002.16 g, DODI 5200.48 (3.10), NIST SP 800-171 3.13)				
Are there procedures in place for handling CUI when it needs to be faxed including the receiver has been notified by the sender? (32 CFR 2002.16 g, DODI 5200.48 (3.10), NIST SP 800-171.3.10.1)				
Have procedures been established to ensure unclassified copiers and printers connected to the internet are not used for CUI reproduction unless certified for CUI? (32 CFR 2002.16 g, DODI 5200.48 (3.10), NIST SP 800-171 3.4.2)				

8. REPRODUCTION

Similar to other information requiring safeguarding, there are rules regarding reproduction of CUI. While the points below highlight this requirement, one should consult DODI 5200.48 for a more comprehensive description. Authorized holders may reproduce CUI in accordance with distribution statements and applicable laws.

Below are some considerations for establishing a CUI program. Ensure the CUI Manager implements the following as it relates to reproduction of CUI:

REVIEW ITEM	Yes	No	N/A	Notes
Are there procedures established to oversee and control the reproduction of CUI material. (32 CFR 2002.14.e, DODI 5200.48 (5.1))				
Are only approved printers and copiers used for CUI reproduction? (32 CFR 2002.14.e, DODI 5200.48 (5.1))				
Are personnel, who reproduce CUI, aware of the risks involved with the specific reproduction equipment and the appropriate countermeasures they are required to take? (32 CFR 2002.14.e, DODI 5200.48 (5.1))				
Are all waste products generated during reproduction properly protected and disposed of? (32 CFR 2002.14.e, DODI 5200.48 (5.1))				
Is reproduction equipment specifically designated for the reproduction of CUI material? (32 CFR 2002.14.e, DODI 5200.48 (5.1))				

9. DISPOSITION AND DESTRUCTION

Similar to other information requiring safeguarding, there are rules for destruction of CUI. While the points below highlight these requirements, one should consult DODI 5200.48 for a more comprehensive description. If there is no longer a use for CUI documents or materials, all hard and soft copies should be destroyed rendering them unreadable, indecipherable, and irrecoverable.

Below are some considerations for establishing a CUI program. Ensure the CUI Manager implements the following as it relates to destruction of CUI:

REVIEW ITEM	Yes	No	N/A	Notes
Are CUI documents and materials properly reviewed for disposition status determination? (32 CFR 2002.14.f, DODI 5200.48 (4.5))				
Are CUI documents and materials properly destroyed by approved methods? (32 CFR 2002.14.f, DODI 5200.48 (4.5))				
Is each program office with CUI holdings setting aside at least one “Clean Out” day each year when specific attention and effort is focused on disposition of unneeded/temporary CUI material? (32 CFR 2002.14.f, DODI 5200.48 (4.5))				

10. TRANSMISSION AND TRANSPORTATION

CUI materials in paper or media format can be sent via first class mail, parcel post, or bulk shipments. CUI can also be transmitted by e-mail when practical, via approved secure communication systems or systems using other protective measures.

Below are some considerations for establishing a CUI program. Ensure the CUI Manager implements the following as it relates to transmission and transportation of CUI:

REVIEW ITEM	Yes	No	N/A	Notes
Is CUI transmitted outside of your facility safeguarded with at least one layer of protection or similar wrappings or containers durable enough to properly protect the material from accidental exposure and facilitate detection of tampering? (32 CFR 2002.14.d, DODI 5200.48 (5.1))				
Are proper procedures used when mailing CUI? (32 CFR 2002.14.d, DODI 5200.48 (5.1))				
Are there procedures in place to notify security when CUI is removed from the work environment? (32 CFR 2002.14.d, DODI 5200.48 (5.1))				
Are there procedures established to limit the hand-carrying of CUI to only when other means of transmission or transportation cannot be used? (32 CFR 2002.14.d, DODI 5200.48 (5.1))				
Are all hand-carrying officials briefed on and have they acknowledged their responsibilities for protecting CUI? (32 CFR 2002.14.d, DODI 5200.48 (5.1))				

11. SECURITY EDUCATION AND TRAINING

CUI security education and training is required when requested by the Government Contracting Activity for contracts with CUI requirements. The Center for Development of Security Excellence (CDSE) has created a CUI training course that meets the requirements of the DODI 5200.48 and is located at https://securityawareness.usalearning.gov/cui/index.html.

This course is mandatory training for all DOD personnel with access to CUI. The course provides information on the eleven training requirements for accessing, marking, safeguarding, decontrolling, and destroying CUI along with the procedures for identifying and reporting security incidents. This course also fulfills CUI training requirements for Industry when it is required by Government Contracting Activities for contracts with CUI requirements. Contractors may also develop their own training if it contains the mandatory elements outlined in CUI Notice 2016-01.

Below are some considerations for establishing a CUI program. Ensure the CUI Manager implements the following as it relates to your CUI program:

REVIEW ITEM	Yes	No	N/A	Notes
Has the CUI Manager established an effective CUI Oversight Security Education program? (32 CFR 2002.30.a, DODI 5200.48 (3.6)b)				
Have all personnel been trained on policies for CUI identification, safeguarding, and decontrolling? (32 CFR 2002.30.a, DODI 5200.48 (3.6)g)				
Has refresher training been provided at least annually to assigned employees? (32 CFR 2002.30.a, DODI 5200.48 (3.6)b)				
Are records maintained to show the names of employees who participated in "initial" and “refresher” training? (32 CFR 2002.30.a, DODI 5200.48 (3.6)b)				
Is CUI training included in new employee orientations? (32 CFR 2002.30.a, DODI 5200.48 (3.6)b)				

12. SECURITY INCIDENTS AND MISUSE OF CUI TO INCLUDE COMPROMISES

The DODI 5200.48 defines a misuse of CUI as an occurrence that takes place when someone uses CUI in a manner not in accordance with the policy contained in the E.O. 13556, 32 CFR 2002, the CUI Registry, agency CUI policy, or the applicable laws, regulations, and Government-wide policies that govern the affected information. This may include international 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. An Unauthorized Disclosure (UD) is described as communication or physical transfer of classified or CUI to an unauthorized recipient. Industry is to report misuse, mishandling, or UD of CUI to the DCSA ESO Office mailbox at dcsa.quantico.ctp.mbx.eso-cui@mail.mil. DCSA is creating a "Misuse of CUI Reporting" job aid & "CUI UD Reporting" job aid that will give further guidance on reporting requirements of both misuse of CUI incidents and UDs. When finalized, the job aids will be available at https://www.dcsa.mil/mc/ctp/cui/.

Below are some considerations for establishing a CUI program. Ensure the CUI Manager implements the following as it relates to security incidents and misuse of CUI:

REVIEW ITEM	Yes	No	N/A	Notes
Are all assigned employees trained on their responsibilities to report security violations concerning CUI? (32 CFR 2002.54, DODI 5200.48 (5.2))				
Are there procedures in place to conduct an inquiry and/or investigation of a loss, possible compromise, or unauthorized disclosure of CUI? (32 CFR 2002.54, DODI 5200.48 (5.2))				
Are appropriate and prompt corrective actions taken when a misuse of CUI violation or infraction occurs? (32 CFR 2002.54, DODI 5200.48 (5.2))				
Are inquiries and/or investigations conducted promptly to ascertain the facts surrounding reported incidents? (32 CFR 2002.54, DODI 5200.48 (5.2))				
Are all individuals who commit misuse of CUI violations or infractions subject to appropriate disciplinary actions? (32 CFR 2002.54, DODI 5200.48 (5.2))				

CURRENT POLICY DOCUMENTS THAT ADDRESS CUI OVERSIGHT

Four main policies govern CUI. The following policy documents can be located at https://www.dcsa.mil/mc/ctp/cui/.

1. **DOD Instruction 5200.48 “Controlled Unclassified Information”**
2. **32 CFR 2002 Part IV National Archives and Records Administration 32 CFR Part 2002 “Controlled Unclassified Information”**
3. **E.O. 13556 Vol 75, No 216. “Controlled Unclassified Information”**
4. **NIST Special Publication 800-171 “Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations”**

CONTROLLED
UNCLASSIFIED
INFORMATION

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