

CUI Managers may find this sample useful when creating their Standard Practice and Procedures (SPP); however, it should be used only as a guide. In order to create an effective CUI Program SPP, the CUI Manager must determine facility-specific requirements and make any necessary modifications to incorporate those facility-specific procedures.

CONTROLLED UNCLASSIFIED INFORMATION (CUI) PROGRAM

Standard Practices and
Procedures (SPP)
Addendum

[FACILITY NAME]

[FACILITY ADDRESS]

Table of Contents

[CUI Definition 2](#_Toc90561074)

[Purpose of SPP and Applicability 2](#_Toc90561075)

[CUI Manager 2](#_Toc90561076)

[Training & Awareness 3](#_Toc90561077)

[Initial Training 3](#_Toc90561078)

[Annual Refresher Training 3](#_Toc90561079)

[Training Records 3](#_Toc90561080)

[Self-Inspection 3](#_Toc90561081)

[CUI Life Cycle 4](#_Toc90561082)

[Creating CUI 5](#_Toc90561083)

[Identifying CUI 5](#_Toc90561084)

[Marking CUI 5](#_Toc90561085)

[Storing CUI 5](#_Toc90561086)

[System and Network Requirements 6](#_Toc90561087)

[Disseminating CUI 6](#_Toc90561088)

[Transmitting CUI 6](#_Toc90561089)

[Destroying CUI 6](#_Toc90561090)

[Decontrolling CUI 7](#_Toc90561091)

[CUI Unauthorized Disclosure and CUI Misuse 8](#_Toc90561092)

[Unauthorized Disclosure 8](#_Toc90561093)

[CUI Misuse 8](#_Toc90561094)

[Handling Responsibilities for Information Owners & End-Users 9](#_Toc90561095)

[Compliance and Acknowledgment 9](#_Toc90561096)

# CUI Definition

* Controlled Unclassified Information (CUI) is unclassified information requiring safeguarding and dissemination controls, consistent with applicable law, regulation, or government-wide policy. There are two designations for CUI – Basic and Specified (SP).
* 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.
* 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 distinction is the underlying authority spells out the controls for CUI Specified information and does not for CUI Basic information.

# Purpose of SPP and Applicability

* The purpose of this document is to define the standards to create, identify, mark, store, disseminate, destroy, and decontrol CUI that [INSERT FACILITY NAME] receives or generates in connection with the performance of government contracts along with the procedures for identifying and reporting security incidents.
* This SPP applies to all employees, subcontractors, consultants, vendors, and visitors to our facility. Additionally, this Standard applies to all information systems that access, process, and/or store CUI.
* This SPP applies to all US Government contracts and subcontracts, and related solicitations where FAR 252.204-7012 is incorporated for the protection of CUI.

# CUI Manager

* [INSERT FACILITY NAME] has appointed a CUI Manager to manage the facility’s CUI Program. The CUI manager:
* Is a US Citizen, and
* Has completed initial CUI training
* The CUI Manager will complete/has completed required training when requested by the Government Contracting Activity (GCA) for contracts with CUI requirements and is responsible for developing and implementing security guidance necessary for CUI program implementation. Training is required annually for Department of Defense (DOD) contracts and bi-annually for non-DOD contracts.
* [INSERT CUI MANAGER NAME] is the CUI Manager for [INSERT FACILITY NAME] and can be reached at [INSERT CUI MANAGER CONTACT INFORMATION].

# Training & Awareness

## Initial Training

* All employees that handle CUI as part of their duties should complete required training when requested by the Government Contracting Activity (GCA) for contracts with CUI requirements.
* Per DoDI 5200.48, DOD contractors require initial training and annual refresher training on CUI.
* Industry should note that this requirement is different from agencies governed by 32 CFR 2002, which requires refresher training every two years.
* The Defense Counterintelligence and Security Agency (DCSA) Center for Development of Security Excellence (CDSE) provides CUI training that is available to industry (IF141.06). The course fulfills CUI training requirements for industry when it is required by Government Contracting Activities for contracts with CUI requirements (and for all employees that handle CUI as part of their duties).

## Annual Refresher Training

(INSERT FACILITY NAME) will provide annual refresher training to all employees handling CUI in order to remind employees of their obligation to protect CUI and provide any updates to security requirements.

## Training Records

The CUI Manager will maintain records showing names of employees who have taken the initial and refresher training, the method of course delivery, and the date of completion.

# Self-Inspection

The CUI Manager will review the CUI Self-Inspection Appendix to assist in the initial establishment of (INSERT FACILITY NAME’s) CUI Program. Once established, the CUI Self-Inspection Appendix should be considered to self-assess the CUI security procedures, determine compliance, and effectiveness of (INSERT FACILITY NAME’s) CUI Program, and identify any deficiencies/weaknesses. The self-inspection results must be documented. The results of the self-inspection will be briefed to employees during refresher training.

# CUI Life Cycle

CUI follows a life cycle similar to all protected information. While the designation of certain types of information requiring safeguarding and dissemination may be new, the process should be very familiar.

***CUI Life Cycle Graph***

## Creating CUI

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

## Identifying CUI

* The CUI Manager will review existing contracts and engage with Government customers to determine which, if any, CUI requirements are applicable to current contracts.
* The CUI Manager will review the National CUI Registry at <https://www.archives.gov/cui> to become familiar with CUI organizational index groupings and CUI categories and will check the registry periodically for updates.
* Whenever the government provides new information to (INSERT FACILITY NAME), it must identify whether any of the information is CUI via the contracting vehicle and mark such documents, material, or media with required CUI markings.

## Marking CUI

* 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. Marking requirements apply to documents, emails, and forms of media that are designated as CUI.
* Marking labels are available for media such as USB sticks, hard drives, and CD ROMs to alert holders to the presence of CUI stored on the device in accordance with NARA ISOO CUI Notice 2019-01. The labels can be found in the DOD CUI Marking Guide. The National Industrial Security System (NISS) is currently authorized to process and store CUI.

## Storing CUI

* (INSERT FACILITY NAME) employees will only utilize authorized, (INSERT FACILITY NAME) owned, and managed networks, domains, information systems, and media for the transmission, processing, and storage of CUI.
* During working hours, (INSERT FACILITY NAME) must take steps to minimize the risk of access by unauthorized personnel, such as not reading, discussing, or leaving CUI unattended where unauthorized personnel are present.
* After working hours, (INSERT FACILITY NAME) must ensure that CUI is stored in unlocked containers, desks, or cabinets if the building provides security for continuous monitoring of access. If building security is not provided, then CUI information must be stored in locked desks, file cabinets, bookcases, locked rooms, or similarly secured areas.
* CUI should never be placed on externally owned, publicly accessible websites.

### System and Network Requirements

(INSERT FACILITY NAME) must ensure that all information systems that transmit, process, or store CUI meet the NIST 800-171 information security requirements to adequately protect CUI on non-federal information systems.

## Disseminating CUI

* Disclosure of CUI is limited to those with a lawful government purpose and to those that, prior to the disclosure of the CUI, are capable of providing adequate security of the CUI. This means that if CUI will be disseminated physically or electronically, (INSERT FACILITY NAME) personnel must ensure, prior to transmission of the CUI, that the receiver’s information systems processing, storing, or transmitting CUI provide adequate security.
* 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.
* Unauthorized disclosure (UD) is when CUI is disclosed to someone without a lawful government purpose or to someone incapable of providing adequate security over the CUI. A UD is described as communication or physical transfer of classified or CUI to an unauthorized recipient. The CUI Manager must report UD of CUI to the DCSA Enterprise Security Operations (ESO) Office mailbox at
dcsa.quantico.ctp.mbx.eso-unauthorized-disclosure@mail.mil.

### Transmitting CUI

* CUI material may be transmitted via first class mail, parcel post, or bulk shipments.
* When practical, CUI 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 (PKI) or transport layer security (e.g., HTTPS).
* 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).

## Destroying CUI

When destroying CUI, including in electronic form, the CUI Manager must ensure this is done so in a manner making it unreadable, indecipherable, and irrecoverable.

## Decontrolling CUI

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.

# CUI Unauthorized Disclosure and CUI Misuse

## Unauthorized Disclosure

UD is when CUI is disclosed to someone without a lawful government purpose or to someone incapable of providing adequate security over the CUI. A UD is described as communication or physical transfer of classified or CUI to an unauthorized recipient. The CUI Manager must report UD of CUI to the DCSA ESO Office mailbox at dcsa.quantico.ctp.mbx.eso-unauthorized-disclosure@mail.mil.

## CUI Misuse

* Misuse of CUI is 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.
* When a CUI misuse occurs, the CUI Manager is responsible for conducting a preliminary Administrative Inquiry (AI). The purpose of the preliminary inquiry is to secure the CUI information, quickly gather the available facts, and determine if CUI information was subject to compromise. If the CUI Manager concludes, based on the preliminary AI, that no loss, compromise, or suspected compromise occurred, the CUI Manager has the responsibility to finalize the inquiry.

# Handling Responsibilities for Information Owners & End-Users

* All (INSERT FACILITY NAME) employees are responsible for the content they create or send over company email, internet, or text.
* All CUI must be access-controlled for authorization and limited to individuals who possess a lawful government purpose to access the information.
* CUI must only be transferred to locations, persons, and entities that meet the requirements to provide adequate security for CUI.
* All CUI digitally sent must be encrypted using authorized tools and/or solutions.
* CUI must never be accessed from, processed on, transmitted from, or stored on public computers (i.e., internet kiosks, airports, hotel business centers, etc.)
* When working with CUI, it is required to establish a controlled environment that will safeguard CUI. Therefore, to access or store CUI in an authorized mobile phone or tablet, the device must adhere to CUI safeguarding contractual requirements
* CUI must not be sent via text message capabilities (SMS).
* CUI must not be captured via personal camera from any source (e.g., whiteboard).

# Compliance and Acknowledgment

Employees of (INSERT FACILITY NAME) understand the end-user responsibilities to identify, handle, process, and protect CUI in the performance of their duties and in performance of a government contract and that non-compliance with this Standard may result in disciplinary measures up to and including termination of employment.

Employees of (INSERT FACILITY NAME) should contact the CUI Manager if there are any questions about any of the sections in this document.