Controlled Unclassified Information
GSA CUI Guide

This Controlled Unclassified Information (CUI) Guide is designated as policy per GSA Order CIO 2103.1 Controlled Unclassified Information (CUI) Policy

Controlled Unclassified Information (CUI) Guide

Table of Contents

Purpose

GSA's CUI policy and this CUI Guide implement Executive Order 13556, Controlled Unclassified Information (CUI), and the requirements of 32 C.F.R. Part 2002, and establish policy and framework for the CUI Program at GSA. CUI is defined as unclassified information that requires safeguarding and dissemination controls pursuant to law, regulation, or government-wide policy, as listed in the CUI Registry by the Executive Agent (EA), the National Archives and Records Administration (NARA). NARA has delegated this authority to the Director of the Information Security Oversight Office (ISOO).

The CUI Program is designed to address several deficiencies in managing and protecting unclassified information, including inconsistent markings, inadequate safeguarding, and needless restrictions, both by standardizing procedures and by providing common definitions through a CUI Registry.

This Guide sets forth the GSA framework for incorporating CUI requirements into GSA's processes for handling unclassified information that requires safeguarding and dissemination controls as required by law, regulation, and government-wide policy. This Guide furthers GSA Order CIO 2103.1 Controlled Unclassified Information (CUI) Policy by providing specific details concerning the implementation and maintenance of the CUI Program at GSA. This Guide does not apply to uncontrolled unclassified information or to classified information.

Background

Executive Order 13556 *Controlled Unclassified Information* establishes an open and uniform program to standardize the way executive branch agencies handle information that requires protection but is not classified. In the past this information was not handled and marked consistently by all executive branch agencies and there was no government-wide direction on what information should be protected. The CUI Program reduces confusion by establishing uniformity across the executive branch in how sensitive but unclassified information will be identified, marked, accessed, disseminated, safeguarded, decontrolled, and destroyed.

Under the CUI Program, the only types of information that may be marked and handled as CUI are those identified in the CUI Registry and covered by applicable laws, regulations or government-wide policies. The CUI Program regulates the type of information that can and should be protected as shown in the CUI Registry. The CUI Program also incorporates a process that all executive branch agencies will utilize to protect and share sensitive information.

Part 2002 of Title 32 of the Code of Federal Regulations defines how the CUI Program will be implemented in the executive branch. The CUI Executive Agent has established a CUI Registry at archives.gov/cui that serves as the authoritative reference for all CUI categories, authorities, markings, and other information.

Implementation

There will be a phased implementation of the CUI Program within GSA and the executive branch. The date of full implementation of the Program will be announced when known, with periodic communications providing updates. See InSite.gsa.gov/cui for current information.

Throughout implementation, legacy markings and associated safeguarding practices will exist at the same time, but as implementation progresses, legacy markings and their safeguarding practices will be phased out.

Responsibilities

All personnel working in or with GSA must be aware of required CUI protections and complete all mandatory training. Specific responsibilities for positions and organizations are defined in CIO 2103.1 GSA CUI Policy.

The CUI Registry

The CUI Registry serves as the Government-wide central repository for all information, guidance, policy, and requirements on handling CUI, including authorized CUI categories, associated markings, handling, and decontrolling procedures.

Existing policies for managing unclassified information that is sensitive (SBU, PII, etc.) remain in effect until GSA implements the CUI Program. See “Sending and Receiving CUI During the Implementation Process” later in this Guide for dealing with other agencies who are at different stages of CUI Program implementation.

- The CUI Executive Agent (National Archives and Records Administration (NARA)) maintains the CUI Registry and the associated website: archives.gov/cui.

- The CUI categories explain the 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 EA has approved and listed in the CUI Registry, and shall serve as exclusive designations for identifying CUI.

- All controlled unclassified information that qualifies as CUI must be handled within the parameters of the CUI Program and marked appropriately per the CUI Registry.

- Items can only be marked according to the CUI Registry. And only items that fall under the purview of the CUI Registry may be marked as CUI.

- The CUI Registry includes citations to laws, regulations, or government-wide policies that form the basis for each category, and notes any sanctions or penalties for misuse of each

category. If there is a need to add a CUI category to the CUI Registry, there must be a corresponding authority that says the item will and should be protected.

- No uncontrolled information may be labeled as CUI. If there is a need to add a CUI category (see the Definitions section of this Guide) to the CUI Registry, there must be a corresponding authority that says the item can and should be protected. Contact the GSA CUI Program Manager for assistance.

Identifying CUI

- Controlled Unclassified Information (CUI) is information the Government creates or possesses that a law, regulation, or government-wide policy requires or specifically permits an agency to handle by means of safeguarding or dissemination controls. CUI also includes data created by contractors operating Federal Information Systems on behalf of the Government. A Federal Information System as defined in GSA Order CIO 2100.1 IT Security Policy as “an information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency". A GSA information system is an example of a federal information system.

    - Examples of sensitive or protected information that are now being replaced by CUI markings and will no longer be allowed once CUI is fully implemented, include Sensitive But Unclassified (SBU), Confidential, Private, For Official Use Only (FOUO), and other less common markings that may be in use. Personally Identifiable Information (PII), while now a subset of CUI, may still be referred to as PII in accordance with the Privacy Act.

    - For a complete listing of CUI Categories, refer to the CUI Registry on NARA’s webpage (archives.gov/cui).

- The owner of the information makes the determination as to whether or not information is CUI. Those owners who create and manage such data must be very familiar with the CUI categories and CUI policies, complete all training, and know how to determine what information is CUI and how it should be handled (see InSite.gsa.gov/cui for information). They will determine the type of CUI (Basic or Specified -- see “Safeguarding Standards” below, and the “Definitions” section of this Guide), the applicable category, and the necessary markings and decontrol actions required based on the specifics within this Guide. See the list of Categories likely used by GSA with associated markings.

- The current PBS policy PBS 3490.3 Security for Sensitive Building Information Related to Federal Buildings, Grounds, or Property governs handling of sensitive information specifically focused on building drawings. The terminology within that policy has been updated to coincide with the CUI Program and it should be consulted, along with the GSA CUI Policy and this Guide, when dealing with sensitive building information that must be

protected. The CUI category for this information will be Physical Security as found in the CUI Registry.

- CUI official documents may be GSA records. If they are determined to be records they must not be destroyed until applicable records retention has been met and any applicable litigation hold has been lifted. See OAS 1820.1 P GSA Records Management Program for additional information on managing records. (One example: convenience copies of documents marked CUI should be protected as CUI, but would not be records.) CUI papers must be destroyed in an approved shredder that shreds to 1x5mm or into a locked bin marked as approved for CUI. See the Destruction section of this guide for details and for information on destroying electronic media.

- The GSA CUI Program does not apply to classified information which is governed by Executive Order 13526 - Classified National Security Information. No classified information may be controlled within the CUI Program.

Safeguarding CUI

General Safeguarding Policy.

- CUI, regardless of its form, shall be protected at all times in a manner that minimizes the risk of unauthorized disclosure while allowing for access by authorized holders.

- Authorized holders of CUI are responsible for complying with applicable safeguarding requirements in accordance with 32 CFR 2002, this Guide, and all applicable guidance published in the CUI Registry.

- All sensitive information should be protected even if the markings are incorrect or missing. Due to varied time spans that agencies will transition from legacy markings to CUI, some sensitive information may not be marked properly, or may not be marked at all. This information should still be treated and safeguarded as CUI. Anyone finding an incorrectly marked document should notify the disseminating individual or agency and request a properly marked document, or have them confirm that it is not CUI.

- For categories specifically designated as CUI Specified, holders must follow the procedures in the underlying laws, regulations, or government-wide policies that established the specific category involved. This information is available in the CUI Registry.

Safeguarding Standards. Users must safeguard CUI using one of two types of standards, CUI Basic or CUI Specified.

- **CUI Basic** is the default set of CUI categories that must be applied to all CUI unless the CUI Registry requires CUI Specified. CUI Basic differs from CUI Specified in that, although laws, regulations, or government-wide policies require agencies to protect or

control the CUI Basic information, they do not specifically articulate any safeguarding or dissemination controls for that information. The CUI Basic controls therefore apply whenever CUI Specified ones do not cover the involved CUI.

- **CUI Specified** is the set of CUI categories whose supporting law, regulation, and/or government-wide policy require specific safeguarding measures that are more stringent than, or otherwise differ from those required for CUI Basic.

(a) Only categories designated in the CUI Registry as CUI Specified may impose these more stringent safeguarding measures.

(b) Only CUI categories the CUI Executive Agent approves and designates in the CUI Registry as CUI Specified may apply specified controls rather than CUI Basic controls.

(c) When an authority for a CUI Specified category is silent on either safeguarding or dissemination of the involved CUI, agencies must apply CUI Basic controls.

(d) 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 categories and does not for CUI Basic ones.

Safeguarding Practices.

- Only authorized holders shall have access to CUI. An authorized holder is a person or entity that handles GSA's CUI, has completed the required CUI training, and has authorization from GSA management to designate or handle CUI (also see Definitions section).

- CUI in printed copy must be kept under direct control of an authorized holder, protected by at least one physical barrier, for example, stored behind a locked door, drawer, or file cabinet whenever it is left unattended. Even where the facility/building is secure, CUI must not be left unattended in open office areas.

- All CUI must be protected from access, overhearing, or observation by unauthorized persons. In GSA's open office environments CUI holders should be aware of CUI being seen on the computer screen, should find a private area for CUI-related discussions, and may use a CUI cover sheet (see below for details).

- When outside a GSA building or other controlled environment, personnel must keep CUI under their direct control at all times or protect it with at least one physical barrier, and reasonably ensure that they, or the physical barrier, protect the CUI from unauthorized access or observation. CUI shall not be viewed while on public transportation or open areas where others may be exposed to it. In hotel rooms, CUI should be kept in a locked briefcase or room safe. While not a good practice, CUI could be stored in a locked

automobile if absolutely necessary, but only if it is in an envelope, briefcase, or otherwise covered from view, and best locked in the trunk.

- Reproduction of CUI (copying, faxing, scanning, printing, electronic duplication) is allowed if in furtherance of a lawful government purpose.

    - CUI documents should not be left on a printer, they should be removed as soon as printed.
    - Faxing of CUI documents is authorized provided the recipient has a lawful government purpose for access.
    - Authorized holders who fax documents should confirm the authorized recipient is available to receive, and did indeed receive the fax.

- Authorized interoffice or interagency hardcopy mail systems and electronic systems may be used to transport/transmit CUI. See Methods of Disseminating CUI section of this Guide.

- Envelopes or packages that contain CUI should be marked to indicate that they are intended for the recipient only and should not be forwarded. No CUI markings should be placed on the outside of an envelope or package.

- Electronic CUI shall only be stored in a password protected system (e.g., database, email, network drive, website, segregated and protected electronic storage device). See the section below for more details.

- Authorized holders must ensure that all persons involved in CUI discussions or meetings are authorized to receive CUI before using voicemail systems, messaging or chat functions, telepresence systems, video teleconferencing, or any other electronic means of sharing.

- When transporting CUI to and from an alternate work location, the information must be protected as specified in this Guide (See the Methods of Disseminating CUI section of this Guide).

- Refer to IT Security Procedural Guide Media Protection [CIO IT Security 06-32] for details on protection of and controlling access to digital and hardcopy information, and sanitization of media prior to disposal or reuse. IT Procedural Guides can be found on InSite.

Safeguarding CUI in Federal and Non-Federal Systems.

- See the Definitions section for a full explanation of Federal and Non-Federal Systems.

- All applicable GSA policies apply when CUI is held within an IT system. Additional guidance can be found in CIO-IT Security Procedural Guides. The guides provide more detailed information on how to implement security processes and controls and provide worksheets and forms to meet reporting requirements. The guides are updated as needed to reflect the latest regulations and technologies.

- All applicable government-wide standards and guidelines issued by the National Institute of Standards and Technology (NIST), and applicable policies established by the Office of Management and Budget (OMB) apply (see FIPS Publication 199, FIPS Publication 200, and NIST SP 800– 53). A current list of government-wide security guidance is located at http://www.nist.gov/publication-portal.cfm.

- CUI is categorized at the moderate confidentiality impact value in accordance with FIPS Publication 199. Systems that include CUI must incorporate the requirement to safeguard CUI at the moderate confidentiality impact value into their design and management actions. GSA may increase the confidentiality impact value above moderate and apply additional security requirements and controls *only internally* and may not require anyone outside the agency to maintain the higher impact value or more stringent security requirements/controls.

- Electronic CUI shall only be stored in a password protected system (e.g., database, email, network drive, segregated and protected electronic storage device). CUI indicators must be present to alert users of the presence of CUI within the system. The warning could be shown on the login screen, via a screen after logging in, and/or in headers that appear on each screen.
    - Apply banner marking to outputs when printing
    - Use filename indicator (e.g., [contains CUI])
    - CUI cover sheet (upon printing)
    - Splash screen (upon log in or initial access to system)
    - Individual pages can carry a banner marking to indicate CUI is present

- CUI shall not be processed on personally owned electronic devices unless connected through an approved GSA system with approved controls in place. CUI shall not be stored on personally owned electronic devices.

- CUI shall not be sent to or from personal email accounts.

- CUI shall not be posted on or processed through any external or non-agency approved websites or portals (internet kiosks, social media sites, blogs, etc.).

- NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, addresses the elements necessary to protect CUI on non-Federal information systems in accordance with the requirements of 32 CFR 2002.

Marking CUI

General.

- All CUI documents must be marked and protected according to applicable laws, regulations, and government-wide policies. CUI markings listed in the CUI Registry are the only markings authorized to designate unclassified information requiring safeguarding or dissemination controls.

- Authorized holders of CUI will be held accountable for knowing and following these procedures as described in the mandatory training and this Guide. Authorized holders may determine what information qualifies for CUI status and apply the appropriate CUI markings when the information is designated as CUI.

- CUI markings must not be used to conceal illegality, negligence, ineptitude, or other disreputable circumstances embarrassing to any individual, any agency, the Federal Government, or any of their partners, or for any purpose other than to adhere to the law, regulation or government-wide policy authorizing the control.

- Anyone finding an incorrectly marked document should notify the disseminating individual or agency and request a properly marked document, or have them confirm that it is not CUI. The lack of CUI markings on information that qualifies as CUI does not exempt the authorized holder from abiding by applicable handling requirements as described in Executive Order 13556, 32 CFR Part 2002, and the CUI Registry. Also see the “Incident Management” section of this Guide.

Banner Markings.

- Except under certain circumstances, all CUI must be marked with a CUI banner marking at the top of each page (banner markings are also authorized as optional at the bottom of each page, but they are not required for GSA). The content of the banner marking must be inclusive of all CUI within the document and must be the same on every page. If the document contains only CUI Basic, the banner may consist of just the letters CUI. If the document contains CUI Specified, the full marking must be used to indicate the type of CUI and the dissemination controls if any.

- Banner markings may include up to three elements:

    - CUI control marking (mandatory for all CUI). Agencies have the choice of using either the word CONTROLLED or the initialism CUI as the control marking. This marking is mandatory for all CUI and, by itself, is sufficient to indicate the presence of CUI Basic categories. GSA is choosing to standardize on the marking CUI. The reference to CONTROLLED is just for informational purposes since other agencies may use it.

- CUI category marking (mandatory for CUI Specified). If any part of a document contains CUI Specified, then the applicable category marking must appear in the banner, preceded by a "SP-" to indicate the specified nature of the category (e.g., CUI//SP-PRVCY). The CUI control marking and any category markings are separated by a double forward slash (//). When including multiple categories in the banner they must be alphabetized, with specified categories appearing before any basic categories. Multiple categories in a banner line must be separated by a single forward slash (/). Refer to the CUI Marking Handbook for more details.

- Limited Dissemination Control Markings. NARA has published a list of several Limited Dissemination Control Markings that can be applied. Limited Dissemination Control Markings are preceded by a double forward slash (//) and appear as the last element of the CUI banner marking. Limited Dissemination Control Markings may only be applied to CUI to bring attention to any dissemination control called for in the underlying authority or to limit the dissemination of CUI. Limited Dissemination Control Markings should be used only after carefully considering the potential impacts on the timely dissemination of the information to authorized recipients.

- The content of the CUI banner marking must apply to the whole document (i.e., inclusive of all CUI within the document) and must be the same on each page of the document.

- All documents containing CUI must indicate the agency of designation. This may come in several forms, including letterhead, signature block, or "controlled by" line, preferably on the first page of the document. A best practice is also to include information for a point of contact, office, or division within the organization.

Marking Guidelines.

- Refer to the CUI Registry and CUI Marking Handbook for detailed information on markings and marking requirements.

- Markings for Categories that GSA is likely to use and links to specific information concerning them is consolidated in a spreadsheet for authorized holders' reference.

Cover Sheets

The CUI cover sheet can be used to identify CUI, alert observers from a distance that CUI is present, and serve as a shield to protect the CUI from inadvertent disclosure. CUI Cover sheets are optional but encouraged when dealing with printed materials since they can help ensure anyone who sees or receives the information is aware of the protection it requires.

Cover sheets (or transmittal letters if faxing), can be used in lieu of banner markings when it is impractical to individually mark every page due to its quantity, legacy status, or the nature of the information. They may be used internally and when transmitting CUI to external entities. However, a CUI Waiver must be obtained from the SAO to allow this departure from normal procedure.

The cover sheet or transmittal letter must:

- Include a designation indicator;
- Convey the status as CUI;
- List any CUI Specified Categories contained in the document or transmission;
- List any applicable Limited Dissemination Controls (markings); and
- List any special handling or dissemination requirements called for by the underlying law, regulation, or Government wide policy related to the CUI Specified information.
- State that if the enclosure is removed the document does not contain CUI.

The CUI cover sheet (Standard Form 901) is available through GSA's forms library or at https://www.archives.gov/cui/additional-tools.

Emails.

- When marking emails, it is mandatory to include the appropriate banner marking to indicate that the email contains CUI. If the email is forwarded, the banner marking must be carried forward.
- It is best practice to include an Indicator Marking such as [Contains CUI]at the end of the subject line.
- If sending an attachment that contains CUI, the name of the file can contain a CUI indicator such as [Contains CUI]. The attachment file must be encrypted using a FIPS-compliant method.
- When sending an email where the attachment is removed and the email no longer contains CUI, add the following statement below the banner marking "When attachment is removed, this email is Uncontrolled Unclassified Information".

Portion Marking.

- Portion marking is a means to provide information about the sensitivity of a particular section of text, paragraph, bullet, picture, chart, etc. The markings consist of an abbreviation enclosed in parentheses, usually at the beginning of a sentence or title.

- Portion marking is not required, but it is permitted to facilitate information sharing and proper handling, and to assist FOIA reviewers in identifying the CUI within a large document that may be primarily Uncontrolled Unclassified Information. See the Marking Handbook on the CUI Registry for the description and use of portion markings.

- If portion markings are used in any portion of a document, they must be used throughout the entire document. All portions or sections must be portion marked, even those that do not contain CUI. The paragraphs that contain CUI should begin with the designation (CUI). Sections that do not contain CUI should be marked as Uncontrolled Unclassified Information, designated with a (U).

- When authorized holders include CUI in documents that also contain classified (CNSI) information, the portions must be marked appropriately. The decontrolling provisions of the CUI Program apply only to the portions marked CUI. See the CUI Marking Handbook for specific guidance on commingling CUI with CNSI.

Legacy materials.

- Documents that are currently in use and were created prior to implementation of the CUI Program must be reviewed and marked to reflect appropriate CUI controls.

- When legacy documents, or information from them, are to be reused, they must be re-evaluated to determine if CUI protection is needed, and then marked as CUI.

- If requested, the CUI SAO may grant a limited waiver if re-marking is considered prohibitively burdensome.

    - The information must still be safeguarded and disseminated according to CUI procedures. If the information is disseminated outside GSA, the waiver will not apply and the information must be marked with appropriate CUI markings, or through use of a CUI cover sheet or transmittal document, or CUI indication if disseminating via email.

    - When requesting a waiver, include details as to the alternative protection methods that will be employed to ensure protection of the CUI in question.

    - See the Waivers of CUI Requirements section of this Guide for additional information.

Challenges to Designation of Information as CUI.

- Authorized holders of CUI who, in good faith, believe that its designation as CUI is improper or incorrect, or who believe they have received unmarked CUI, should send an email to cui@gsa.gov for internal handling or for notifying the designating agency.

- GSA's SAO will accept and manage challenges to CUI status following this process:

    - The challenge will be emailed to the SAO as soon as it is received.

    - The SAO will acknowledge receipt of the challenge within 7 days by writing (via email or letter, as appropriate) to the challenger or the challenger's agency if the exact person is not known. This response will include the anticipated timetable for response and the contact information for the SAO or designee making GSA's decision.

    - The SAO will provide the challenger the opportunity to explain, verbally or in writing, their rationale for believing the CUI is inappropriately designated.

    - The SAO will ensure that both internal and external challengers have the option of bringing it anonymously, and that challengers are not subject to retribution.

    - Until the challenge is resolved, all authorized holders must continue to safeguard and disseminate the challenged CUI at the control level indicated in the markings.

    - If a challenging party disagrees with the response to a challenge, that party may use the Dispute Resolution procedures described in 32 CFR 2002.

Working Papers.

Working papers containing CUI must be marked and protected the same way as the finished product and as required for any CUI contained within them. This applies whether or not the working papers will be shortly destroyed, and when no longer needed they should be destroyed as described in the Destruction section of this Guide.

Supplemental Administrative Markings.

Supplemental Administrative Markings (e.g., Pre-decisional, Draft, Deliberative) may be used with CUI but may not impose additional safeguarding requirements or disseminating restrictions. Their purpose is to note the status of documents under development. Supplemental markings may not appear in the CUI banners, nor may they be incorporated into the CUI designating/decontrolling indicators or portion markings. Utilizing watermarks is the best way to display supplemental markings.

Sharing CUI (Accessing and Disseminating)

GSA and all agencies in the executive branch are obligated to ensure that information can be shared with others who have an appropriate need for it in furtherance of a lawful government purpose. These information sharing needs must occur within the parameters of the authorities in the CUI Registry and be balanced by protection requirements. Authorized holders must ensure when sharing CUI that entities who receive it continue protecting it to the required standards.

General Practices.

- Individuals may disseminate and permit access to CUI in accordance with the specific laws shown in the CUI Registry if it furthers a lawful government purpose and is not otherwise prohibited by law.

- Not all sensitive or protected information is automatically considered CUI; only specific applicable information that falls within the categories of the CUI Registry should be controlled as CUI. Unclassified information may not be controlled except through the CUI Program, and access to CUI may not be unlawfully or improperly restricted.

- Prior to disseminating CUI, authorized holders must mark CUI according to the CUI Marking Guide and 32 CFR 2002.

- GSA should enter into a written agreement with any intended non-executive branch entity when possible. For more information on agreements and arrangements with non-executive branch entities see CUI Notice 2018-01.

- When a written agreement is not feasible and CUI must be shared, the authorized holder must communicate to the recipient that the Government strongly encourages the non-executive branch entity to protect CUI in accordance with 32 CFR 2002 and the CUI Registry.

- If an authorized person releases CUI in accordance with an applicable information access statute, such as the Freedom of Information Act (FOIA), the CUI shall remain controlled within GSA and will continue to be handled as CUI.

Controls on Accessing and Disseminating CUI.

- Authorized holders of CUI Basic may disseminate and allow access to any authorized recipient if the requirements of this CUI Guide and 32 CFR 2002 are met.

- Authorized holders of CUI Specified may disseminate and allow access as permitted by the authorizing laws, regulations, or government-wide policies that established that category of CUI Specified (refer to the CUI Registry).

- In the absence of specific dissemination restrictions from the applicable authority, CUI Specified may be disseminated the same as CUI Basic.

- Only the approved dissemination controls in the CUI Registry that limit who CUI may be disseminated to may be used, and only if they serve a lawful government purpose, or are required by law, regulation, or government-wide policy. Refer to the CUI Marking Handbook for further information. If there is significant doubt about whether it is appropriate to use a limited dissemination control, contact the GSA CUI Program Manager at cui@gsa.gov for guidance.

Methods of Disseminating CUI.

- Standard commercially available telephone lines are acceptable for the discussion of CUI, just be aware of the surroundings so unauthorized persons are not within hearing distance.

- CUI on Google sites or GSA webpages shall only be on a restricted site and password protected.

- When sending CUI via email outside of GSA the CUI must be in an encrypted attachment (sending within the GSA network does not require encryption). The body of the email must not contain any CUI, but should include the applicable CUI markings. Attachments shall be encrypted using FIPS-compliant WinZip (see this InSite page for details). Other forms of encryption may be used provided they comply with FIPS 140.

- Holders of CUI shall limit access to CUI to only those individuals authorized to handle it, and shall verify that the information reached its destination. See GSA Order CIO 2100.1 IT Security Policy for additional details.

    - When sending CUI by commercial delivery service or courier, address it to only a specific recipient (not to an office or organization). Automated tracking must be utilized. The US Postal Service or any commercial delivery service may be used to transport CUI as well as any interoffice or interagency mail system.

    - Do not put CUI markings on the outside of the package/envelope.

    - CUI documents shall not be left unattended in an open environment, such as on a printer where unauthorized people can have access to the information.

    - Faxing of CUI documents is authorized provided the recipient has a lawful government purpose for access. Authorized holders must also confirm the authorized recipient is available to receive the fax, and did indeed receive it.

- Follow the requirements for controls on disseminating CUI Basic or CUI Specified as detailed in the CUI Registry for each applicable category.

- When disseminating CUI through a Federal IT system, that system must be in compliance with FISMA requirements and be authorized to operate at the moderate confidentiality impact value (or higher) as set out in FIPS Publications and NIST Guidance. For further information contact the appropriate IT Security Contact.

- Exceptions:

    - CUI Privacy Category - Without written permission from the employee's supervisor, the Data Owner, and the IT system Authorizing Official (AO), authorized holders shall not physically take information marked with one of the CUI **Privacy** Categories from GSA facilities (including GSA managed programs housed at contractor facilities under contract), or access it remotely (i.e., from locations other than GSA facilities unless using GSA approved-systems), in accordance with GSA Order CIO 2100.1 IT Security policy.

    - CUI Physical Security Category - Information marked with CUI's Physical Security Category (e.g., sensitive building information, previously marked Sensitive But Unclassified (SBU)) does not require written permission but the authorized holder should confirm that the receiver has a legitimate building information Lawful Government Purpose for access, as stated in PBS 3490.3 Security for Sensitive Building Information Related to Federal Buildings, Grounds, or Property. If the requestor is unknown to the authorized holder, the authorized holder should contact the designated project manager if the project is in design or construction phase, or the building manager, whichever is responsible for the building/property related to the request for verification. See PBS 3490.3 for details, or for information concerning emergency situations.

Sending and Receiving CUI During the Implementation Process.

While Executive Branch agencies are in various stages of implementing the CUI Program, CUI may be shared, but care must be taken regarding legacy vs. CUI markings.

- Receiving marked legacy information when the recipient has implemented the CUI Program.

    - If the receiving agency plans to reuse or transmit the legacy marked information to another agency, then it must evaluate the information and remark it as CUI as appropriate.

    - If applicable, the receiving agency must also adhere to any agency marking waivers as they apply to internal dissemination.

- If applicable, the receiving agency should apply any appropriate Limited Dissemination Control Markings (LDCMs).
- Receiving agencies should NOT reuse legacy markings, such as FOUO or SBU, on new documents that are derived from marked legacy information.
- Agencies should contact the originator of the material if they have any questions.

- Receiving information marked as CUI when the recipient has NOT implemented the CUI Program.
  - Transmitting agencies may feel some trepidation about the security of their information when sending it to another agency that has not implemented the CUI Program, as the recipient may not inherently protect this information to the same standards outlined in the CUI Program.
  - For this reason, the transmitting agency may wish to directly convey safeguarding requirements for this information to the receiver.
  - Recipients must then protect this information in accordance with any safeguarding guidelines from the originators of the material, individual agency policy, and/or any Limited Dissemination Controls.
  - Receiving agencies should NOT remove CUI markings from the information.
  - Agencies should contact the originator of the material if they have any questions.
- Sending information marked as CUI when the recipient has NOT implemented the CUI Program.
  - The transmitting agency must keep its CUI markings on the information.
  - If CUI Specified or Limited Dissemination Controls are contained in the transmission of the information, the sender should also include a description of the safeguarding or dissemination requirements related to the information.
  - Transmitting agencies may want to use the Optional Form 903 to express these additional safeguards to recipients.
- Sending marked legacy information when the recipient has implemented the CUI Program.

- Transmitting agencies must provide a point of contact with the information in case the recipient has questions about safeguarding the material.

- Any special handling requirements associated with the information, such as limited dissemination controls, should be conveyed through transmittal or in a manner apparent to the recipient of the information..

Decontrolling CUI

- Decontrolling occurs when an authorized holder, consistent with the CUI Registry, removes safeguarding or dissemination controls from CUI that no longer requires such controls. Decontrol may occur automatically or through agency action.

- CUI should be decontrolled (removed from protection of the CUI Program) as soon as practicable when:

  - Laws, regulations, or government-wide policies no longer require CUI controls;

  - An authorized holder from the designating agency requests to decontrol it;

  - The designating agency releases it to the public in response to a FOIA request, which GSA considers to be a public release of the CUI or provides the CUI pursuant to a Privacy Act request (disclosures under the Privacy Act constitute decontrol only with respect to the limited purpose of disclosure to the individual who requested access to their records maintained in a system of records);

  - It is consistent with any declassification action under Executive Order 13526 or any predecessor or successor order; or

  - A predetermined event or date occurs, as described in the authorizing regulations listed in the CUI Registry.

- Decontrolling CUI relieves authorized holders from requirements to handle the information under the CUI Program, but does not constitute authorization for public release.

- Once decontrolled, any public release of information that was formerly CUI must be in accordance with applicable laws and GSA policies on the public release of information.

- Only authorized holders may decontrol CUI.

- The authorized holder must clearly indicate that decontrolled CUI is no longer controlled when restating, paraphrasing, reusing, releasing to the public, or donating

CUI to a private institution. Line through or remove the CUI markings to indicate it is no longer being controlled as CUI.

- Authorized holders may request that a designating agency decontrol certain CUI. If an authorized holder publicly releases CUI in accordance with the designating agency's authorized procedures, the release constitutes decontrol of the information. The authorized procedure should be handled by the CUI SAO. Contact the GSA CUI Program Manager at cui@gsa.gov for information.

- Unauthorized disclosure of CUI does not constitute decontrol. CUI must not be decontrolled solely due to unauthorized disclosure. Proper procedures must still be followed for decontrolling and possible misuse.

- When laws, regulations, or government-wide policies require specific decontrol procedures, authorized holders must follow such requirements.

- Records Management Note: The Archivist of the United States may decontrol records transferred to the National Archives in accordance with 32 CFR Part 2002.34, absent a specific agreement to the contrary with the designating agency.

Decontrolling Indicators

Where feasible, authorized holders must include a specific decontrolling date or event with all CUI. Any decontrolling schedule holding this information should be readily apparent to an authorized holder. The CUI may be decontrolled as of the specific date without further review by the designator. Indicate the date or event when the information can be decontrolled by adding a statement in the footer or elsewhere on the page.

If using an event to authorize decontrol it must be foreseeable and verifiable by any authorized holder. The designator should be the POC and should provide a method of contact for authorized holders to verify that the event has occurred.

Authorized holders must clearly indicate when CUI is no longer controlled. For small documents, all CUI markings within a decontrolled CUI document shall be removed or struck through. For larger documents, removal or strike through of markings can be made on the first page or cover page, and on the first page of any attachments that contain CUI. The first page or cover page should also indicate that the CUI markings are no longer applicable.

Destroying CUI

- CUI may be destroyed when:
    - GSA no longer needs the information; and

    - GSA records disposition schedules no longer require retention of the records. For more information refer to GSA Order OAS 1820.1 GSA Records Management Program.

- Destroy CUI, including in electronic form, in a manner that makes it unreadable, indecipherable, and irrecoverable. CUI may not be placed in office trash bins or recycling containers. CUI must be destroyed as required by the authority for the applicable category. If the authority does not mention a specific method, it should be destroyed according to SP 800-88, Guidelines for Media Sanitization. Specifically, the minimum standard for shredding CUI is to particles that are 1mm x 5mm (.04 inches x .2 inches).

- If a company is contracted with to shred CUI, the contract must ensure protection of the CUI throughout the process, including while in transit and during transfer between collection bins and the shredding equipment. Bins used to collect CUI before being transferred for shredding must be locked and be marked as acceptable for temporarily holding CUI.

- Equipment that is used for the electronic storage or processing of CUI (including copiers, fax machines, scanners, etc.) shall be sanitized per GSA Order CIO 2100.1 IT Security Policy whenever it is transferred, sold, or re-assigned to a person not authorized access to the CUI previously contained in the equipment.

- Since destruction is required by specialized equipment, documents containing CUI information must not be destroyed at an alternate work location (telework location, contractor site, etc.) that doesn't have the proper equipment. CUI must be returned to GSA for destruction in the appropriate shredders or collection bins, or returned to an authorized holder (e.g., a Contracting Officer, the information owner, etc.) for proper destruction.

- Managers and Contracting Officer Representatives (CORs) will periodically review work areas to ensure that sensitive material is being discarded in an appropriate manner.

Transferring records

- When feasible, users must decontrol records containing CUI prior to transferring them to the National Archives and Records Administration (NARA). Refer to Records Management pages on InSite for additional information

- When records cannot be decontrolled before transferring them to NARA, users should work with the local Records Management representative for proper handling.

Training

Employees must receive initial training within 60 days of employment and at least once every 2 years after. The CUI policy delineates the specifics of mandatory training.

Self-Inspection

- In accordance with 32 CFR 2002, GSA must maintain internal oversight efforts to measure and monitor implementation and management of the CUI Program.

- The self-inspection program will include:

    - Self-inspection methods, reviews, and assessments that serve to evaluate program effectiveness, measure the level of compliance, and monitor the progress of CUI implementation;

    - Templates for documenting self-inspections and recording findings;

    - Procedures by which to integrate lessons learned and best practices arising from reviews and assessments into operational policies, procedures, and training;

    - A process for resolving deficiencies and taking corrective actions in an accountable manner; and

    - Analysis and conclusions from the self-inspection program, documented on an annual basis and as requested by the CUI Executive Agent.

- The details and processes of the program will be referenced or included in this Guide when finalized.

Misuse

Misuse of CUI occurs when someone uses CUI in a manner not in accordance with 32 CFR 2002, the CUI Registry, this policy, or the applicable laws, regulations, and Governmentwide 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.

- The CUI SAO is the point of contact for the Executive Agent when the EA receives reports of misuse by GSA from another agency or from within GSA.

- All employees, contractors and lessors shall report suspected or confirmed misuse of CUI as soon as possible. See Incident Management section for more details.

- Where laws, regulations, or government-wide policies governing certain categories of CUI specifically establish sanctions for the misuse of CUI, the SAO is responsible for coordinating with the appropriate parties concerning such sanctions.

- Consequences for misuse of CUI are based on existing GSA policies and the type of information involved (building information, PII, etc.). Each policy's applicable consequences shall apply.

- Consequences for misuse of other agency's CUI shall apply according to GSA policies.

- Any employee who does not comply with this Guide or the laws, regulations, or government-wide policies pertaining to CUI may incur disciplinary action in accordance with HRM 9751.1 Maintaining Discipline.

Sanctions for Misuse of CUI

- Misuse of CUI can result in disciplinary action, up to and including removal from federal service. In the event a contractor employee misuses CUI, the matter shall be referred to the cognizant contracting officer to determine whether remedies should be imposed under the contract.

- When an individual is found to be responsible for the commission of a CUI incident, he/she may be subject to administrative, disciplinary, or criminal sanctions. The underlying law, regulation, or Government-wide policy is consulted to determine guidance on sanctions. The type of sanctions imposed is based on several considerations, including the following:
    - Severity of the incident;
    - Intent of the person committing the incident;
    - Extent of training the person(s) has received;
    - Frequency of which the individual has been found responsible in the commission of other such incidents, to include Security Violations or Infractions involving classified information.
    - Specific requirements in applicable laws, policies or regulations.

- Sanctions include, but are not limited to, verbal or written counseling, reprimand, suspension from duty and pay, removal, removal of access to CUI, or criminal penalties. The underlying law, regulation, or Government-wide policy is consulted for guidance, as appropriate.

- Administrative sanctions are assessed in accordance with the policies, procedures, and practices established by GSA's Office of Human Resources Management, and actions involving the suspension or revocation of a security clearance are taken in accordance with the applicable Executive Orders.

- Where a proposed sanction associated with the unauthorized disclosure of CUI is in excess of a reprimand, the matter is coordinated with the Office of the General Counsel (OGC). Further, where a criminal violation has occurred that may result in a criminal prosecution, the matter is coordinated with OGC, the Office of the Inspector General (OIG), and the Department of Justice.

- The applicability of sanctions is determined without consideration of rank or position.

Incident Management

- An incident can be thought of as a violation (or imminent threat of violation) of security or privacy policies or standard practices. Incidents could cause loss or damage to hardware, software, networks, or data (electronic or hard copy), or could affect personnel. They could be successful or failed attempts to gain unauthorized access to CUI applications, unauthorized entry into a building or room, unauthorized use of a system, unauthorized acquiring or viewing of sensitive data, or similar situations.

- It is crucial to report any such actions or discoveries in order to minimize loss or destruction of information, mitigate weaknesses, restore services, discover the cause of the incident and remedy it, document the incident and GSA's response to it, and to determine any necessary reporting to external sources.

- A potential incident involving CUI that should be reported could come in different forms. Reportable CUI incidents could include but are not limited to:

    - Any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of CUI.

    - Any knowing, willful or negligent action to designate information as CUI contrary to the requirements of Executive Order 13556, and its implementing directives.

    - Any incident involving computer or telecommunications equipment or media that may result in disclosure of CUI to unauthorized individuals, or that results in unauthorized modification or destruction of CUI system data, loss of CUI computer system processing capability, or loss or theft of CUI computer system media.

    - Any incident involving the processing of CUI on computer equipment that has not been specifically approved and accredited for that purpose by an authorized official.

    - Any incident involving the shipment of CUI by an unapproved method, or any evidence of tampering with a shipment, delivery, or mailing of packages containing CUI.

    - Any incident in which CUI is not stored by an approved means.

- Any incident in which CUI is inadvertently revealed to or released to a person not authorized access.
- Any incident in which CUI has been destroyed by unauthorized means.
- Any incident in which CUI has been reproduced without authorization or contrary to specific restrictions imposed by the originator.
- Any incident in which CUI has been shared contrary to an applied dissemination control marking.
- Any other incident in which CUI is not safeguarded or handled in accordance with prescribed procedures.

- Individuals who share CUI external to GSA who become aware of any incident, regardless of whether it did or could have resulted in any actual, potential, or suspected loss or compromise of CUI shall immediately report the incident of misuse to the IT Service Desk. The IT Service Desk will notify the Incident Response Team who will notify the CUI Program Manager. The PM will assist the SAO in determining if the incident of misuse warrants an inquiry and reporting to the Executive Agent.

- GSA Order CIO 2100.1 IT Security Policy and the IT Security Procedural Guide Incident Response (IR) [CIO IT Security 01-02] discuss processes for reporting all types of incidents, and these procedures should be followed for CUI incidents.

- Authorized holders and all GSA employees are responsible for reporting incidents of misuse involving CUI. Specific actions include:
  - **Employees and embedded contractors**: Notify the IT Service Desk at 866-450-5250 or ITServiceDesk@gsa.gov immediately.
  - **Contracts:** Contractors are responsible for reporting incidents in accordance with the requirements of their contract(s). Two Federal Acquisition Regulation (FAR) cases have been opened to incorporate the applicable incident reporting requirements for PII and CUI into the FAR.
  - **Leases:** For building leases involving CUI (previously SBU), the Lessor is responsible for reporting incidents to the Lease Contracting Officer and the GSA Incident Response Team at gsa-ir@gsa.gov.

Waivers of CUI Requirements

When information is designated as CUI but the SAO determines that marking it as CUI is excessively burdensome, the SAO may approve waivers of all or some of the CUI marking requirements while that CUI remains within agency control.

- As stated in CIO 2103.1, GSA CUI Policy, legacy marking of archived documents is not required unless the documents, files, or systems are made active again. The policy grants automatic waivers to CUI marking requirements for legacy material that remains unused. Therefore, if there is a substantial amount of stored information with legacy markings, and removing legacy markings and designating or re-marking it as CUI would be excessively burdensome, a waiver of these requirements for some or all of that information while it remains under agency control, and the information is not being used, is granted.

- In urgent circumstances, the CUI SAO may waive the requirements of the CUI policy or the CUI Registry for any CUI within GSA's possession or control, unless specifically prohibited by applicable laws, regulations, or government-wide policies.

- To allow sharing CUI with other agencies or non-Federal entities or persons in an emergency situation, the SAO may grant an exigent circumstances waiver. In such cases, the authorized holders must make recipients aware of the CUI status of any disseminated information.

- When the circumstances requiring the waiver come to an end, the SAO must reinstitute the requirements for all CUI covered by the waiver without delay.

- The SAO must retain a record of each waiver of CUI requirements, notify authorized recipients and the public of the waivers, and report the waivers to the CUI Executive Agent in the CUI Annual Report.

- To request a waiver contact the SAO at cui@gsa.gov.

Appendix A - References

Executive Order 13556 Controlled Unclassified Information (CUI)	https://obamawhitehouse.archives.gov/the-press-office/2010/11/04/executive-order-13556-controlled-unclassified-information
32 CFR Part 2002 Controlled Unclassified Information (CUI) (Implementing Directive)	https://ecfr.io/Title-32/pt32.6.2002
NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4	https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final
NIST Special Publication, 800-88, Guidelines for Media Sanitization, Revision 1	https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final
NIST Special Publication 800-171 Protecting CUI in Nonfederal Information Systems and Organizations, Revision 1	https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems	https://csrc.nist.gov/publications/detail/fips/199/final
FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems	https://csrc.nist.gov/publications/detail/fips/200/final
FAR Clause 52.204-21, Basic Safeguarding of Contractor Information Systems	https://federalregister.gov/a/2016-11001
Federal Information Security Modernization Act (FISMA)	https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf

GSA Directives

PBS 3490.3 Security for Sensitive Building Information Related to Federal Buildings, Grounds, or Property	https://insite.gsa.gov/directives-library/security-for-sensitive-building-information-related-to-federal-buildings-grounds-or-property-34903-pbs
CIO 1878.1 GSA Privacy Program	https://insite.gsa.gov/directives-library/gsa-privacy-act-program-18781-cio

CIO 2100.1 GSA Information Technology (IT) Security Policy	https://insite.gsa.gov/directives-library/gsa-information-technology-it-security-policy-21001l-cio-chge-1
CIO 2104.1B GSA Information Technology (IT) General Rules of Behavior	https://insite.gsa.gov/directives-library/gsa-information-technology-it-general-rules-of-behavior-21041b-cio-chge-1
CIO 2180.2 GSA Rules of Behavior for Handling Personally Identifiable Information (PII)	https://insite.gsa.gov/directives-library/gsa-rules-of-behavior-for-handling-personally-identifiable-information-pii-21802-cio
CIO 9297.1 GSA Data Release Policy	https://insite.gsa.gov/directives-library/gsa-data-release-policy-92971-cio
CIO 9297.2C GSA Information Breach Notification Policy	https://insite.gsa.gov/directives-library/gsa-information-breach-notification-policy-92972c-cio-chge-1
HRM 9751.1 Maintaining Discipline	https://insite.gsa.gov/directives-library/maintaining-discipline-97511-hrm
OAS 1820.1 P GSA Records Management Program	https://insite.gsa.gov/directives-library/gsa-records-management-program-18201-oas-p
Media Protection Guide [CIO IT Security 06-32]	See IT Security Procedural Guides page on InSite: https://insite.gsa.gov/topics/information-technology/security-and-privacy/it-security/it-security-procedural-guides
Incident Response (IR) [CIO IT Security 01-02]	See IT Security Procedural Guides page on InSite: https://insite.gsa.gov/topics/information-technology/security-and-privacy/it-security/it-security-procedural-guides

Appendix B - Definitions

- Agency (also Federal agency, executive agency, executive branch 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.
- Agreements are arrangements in which agencies set out CUI handling requirements for contractors and other information-sharing partners when the arrangement with the other party involves CUI. Agreements include, but are not limited to, contracts, grants, licenses, certificates, memoranda of agreement or understanding, and information-sharing agreements. When disseminating or sharing CUI with non-executive branch agencies, agencies must enter into written agreements that include CUI provisions whenever possible (see 32 CFR 2002.13(a)(6) and (7) for details). When sharing information with foreign entities, agencies should enter agreements when feasible (see 32 CFR 2002.13(a)(6) and (7) for details).
- Authorized holder is an individual, organization, or group of users that is permitted to designate or handle CUI, in accordance with 32 CFR 2002. Authorized holders who create and manage CUI must be very familiar with the CUI categories and CUI policies, complete all training, and know how to determine what information is CUI and how it should be handled. They will determine the type of CUI (Basic or Specified -- see "Safeguarding Standards" and "Definitions" sections of this Guide), the applicable category, and the necessary markings and decontrol actions required based on the type of information and the specifics within this Guide.
- Classified information is information that Executive Order 13526, "Classified National Security Information," December 29, 2009 (3 CFR, 2010 Comp., p. 298), or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended, requires to have classified markings and protection against unauthorized disclosure.
- 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.
- Control level is a general term that encompasses the category of specific CUI, along with any specific safeguarding and disseminating requirements.
- Controlled Unclassified Information (CUI) is information the Government creates or possesses that a law, regulation, or government-wide policy requires or specifically permits an agency to handle by means of safeguarding or dissemination controls. However, CUI does not include classified information (see definition of classified information, in this section) or information a non-executive branch entity possesses and maintains in its own systems that did not come from an executive branch agency or an entity acting for an agency. Any information, even from non-executive branch entities who are not exclusively included in the CUI Program, identified by federal laws and regulations as being sensitive (e.g.. PII and the Privacy Act) must still be protected appropriately. A law, regulation, or government-wide policy may require safeguarding or dissemination controls in three ways:

- Requiring agencies to control or protect the information but providing no specific controls, which makes the information "CUI Basic" (see definition of CUI Basic in this section);

- Requiring agencies to control or protect the information and providing specific controls for doing so, which makes the information "CUI Specified" (see definition of CUI Specified in this section);

- Requiring agencies to control the information and specifying only some of those controls, which makes the information CUI Specified, but with some CUI Basic controls where the authority does not specify.

- Controls are safeguarding or dissemination requirements that a law, regulation, or government-wide policy requires or permits agencies to use when handling CUI. The requirements may be specifically stated in the authority or the authority may generally require agencies to safeguard the information (in which case, the agency applies the controls from Executive Order 13556, this rule, and the CUI Registry).
- CUI Basic is the set of CUI categories that use the CUI Program's uniform set of controls for handling CUI set forth in this rule. CUI Basic differs from CUI Specified in that, although laws, regulations, or government-wide policies require agencies to protect or control the CUI Basic information, they do not specifically articulate any safeguarding or dissemination controls for that information. The CUI Basic controls therefore apply whenever CUI Specified ones do not cover the involved CUI. (See definition of CUI Specified in this section.)
- CUI categories are those types of information for which laws, regulations, or government-wide policies require agencies to exercise safeguarding or dissemination controls, and which the CUI Executive Agent has approved and listed in the CUI Registry. The controls for CUI Basic categories are the same. However, the controls for CUI Specified categories can differ. If dealing with CUI that falls into a CUI Specified category, review the controls for that category on the CUI Registry. Also consult the agency's CUI policy for specific direction from the Senior Agency Official.
- CUI category markings are the markings approved by the CUI Executive Agent for the categories listed in the CUI Registry.
- CUI Executive Agent 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, 32 CFR 2002, and the CUI Registry.
- CUI Program Manager (PM) 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 2002. Agencies and authorized holders must follow the requirements

in the CUI Registry. Among other information, the CUI Registry identifies all approved CUI categories, provides general descriptions for each, identifies the basis for controls, establishes markings, and sets out handling procedures. The CUI Registry is located on the www.archives.gov/cui/ website (or successor site).

- 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 SAO 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 set of CUI categories that each have specific handling controls required or permitted by authorizing laws, regulations, or government-wide policies. Only CUI categories the CUI Executive Agent approves and designates in the CUI Registry as CUI Specified may apply specified controls rather than CUI Basic ones. When the authorities for a CUI Specified category is silent on either safeguarding or dissemination of the involved CUI, agencies must apply CUI Basic controls to that aspect. 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 categories and does not for CUI Basic ones. (See definition of CUI Basic in this section.)
- Decontrolling occurs when an agency removes safeguarding or dissemination controls from CUI that no longer requires such controls. Decontrol may occur automatically or through agency action.
- Designating CUI occurs when an authorized holder determines that a specific item of information falls into a CUI category. The authorized holder who designates the CUI must make recipients aware of the information's CUI status in accord with 32 CFR 2002.
- Designating agency is the executive branch agency that designates a specific item of information as CUI.
- Disseminating occurs when authorized holders transmit, transfer, or provide access to 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 telephonic 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 that a Federal agency uses or operates, or that a contractor or other non-executive branch entity operates on behalf of an agency. An information system operated on behalf of an agency provides data processing services to the agency that the Government might otherwise perform itself but has decided to outsource. This includes systems operated exclusively for Government use and systems operated for multiple users (multiple Federal agencies or Government and private sector users) such as email services, cloud services, etc. Information systems that are operated by a non-executive branch entity on behalf of an agency are subject to the requirements of 32 CFR 2002 as though they are the agency's systems, and agencies may require these systems to meet additional requirements the agency sets for its own internal systems. A GSA information system is an example of a federal information system.
- Foreign entity is a foreign government, international or foreign public or judicial body, international or foreign private organization (including contractors and vendors), foreign individual (including contractors and vendors), or an element of such an organization that is 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.
- Full Operational Capability (FOC) is attained when all organizations scheduled to receive a system have received it and have the ability to employ and maintain it. For the CUI Program, FOC occurs when policy, training, physical requirements, and IT Systems are all in place and align with the CUI Program. An agency can achieve FOC ahead of the rest of the Executive branch's FOC, and guidance should be provided on how to handle information that is not yet fully CUI compliant.
- Handling is any use of CUI, including but not limited to marking, safeguarding, transporting, disseminating, re-using, and disposing of the information.
- Information owner is the person or office who creates or manages information in hard copy or electronic format, and makes the determination of whether or not information is CUI.
- Initial Operational Capability (IOC) is attained when a capability is available in its minimum usefully deployable form. It is a point in time during the production phase where a system can meet the minimum operational capabilities for a stated need. For the CUI Program, IOC occurs when an agency has their CUI policy in place, has verified physical safeguarding requirements, and has initiated (or completed) training of its workforce.

Some of the older protection practices might still be in place. An agency IOC may be different than an IOC for the entire Executive branch.

- 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.
- 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's existence.
- Limited dissemination is any CUI Executive Agent-approved control on disseminating CUI.
- Misuse of CUI occurs when someone uses CUI in a manner not in accord with the policy contained in Executive Order 13556, 32 CFR 2002, and the CUI Registry, or the applicable laws, regulations, and government-wide policy that establish the affected CUI categories. 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 under a CUI category, or failure to designate or mark information when required per 32 CFR 2002.
- 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; private organizations; or international individuals, including contractors and vendors. This does not include individuals or organizations that may receive CUI information pursuant to federal disclosure laws, including the Freedom of Information Act and the Privacy Act of 1974.
- Non-Federal information system is any information system that does not meet the criteria for a Federal information system. Agencies may not treat non-Federal information systems as though they are agency systems, so agencies cannot require that non-executive branch entities protect these systems in the same manner that the agencies might protect their own information systems. When a non- executive branch entity receives Federal information only incidental to providing a service or product to the Government other than processing services, its information systems are not considered Federal information systems. NIST SP 800–171 (incorporated by reference, see § 2002.2) defines the requirements necessary to protect CUI Basic on non- Federal information systems in accordance with the requirements of this part. Agencies must use NIST SP 800–171 when establishing security requirements to protect CUI's confidentiality on non-Federal information systems (unless the authorizing law, regulation, or Government-wide policy listed in the CUI Registry for the CUI category of the information involved prescribes specific safeguarding requirements for protecting the information's confidentiality, or unless an agreement establishes requirements to protect CUI Basic at higher than moderate confidentiality).
- Personally Identifiable Information (PII) is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information. Because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad. The definition of PII is not

anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified using information that is linked or linkable to said individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information is made publicly available — in any medium and from any source — that, when combined with other information to identify a specific individual, could be used to identify an individual (e.g. SSNs, name, DOB, home address, home email).

- 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 an agency makes information formerly designated as CUI available to members of the public through the agency's official release processes. Disseminating CUI to non-executive branch entities as authorized does not constitute public release; nor does releasing information to an individual pursuant to the Privacy Act of 1974 or disclosing it in response to a FOIA request.
- 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 agreement.
- Re-use means incorporating, disseminating, 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 occurs when individuals or entities, either intentionally or unintentionally, gain access to CUI when such access does not further a lawful government purpose. Unauthorized disclosure may be intentional or unintentional.
- 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 accord 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.