
Directive No: CIO 2158-P-01.1

*Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19*

Controlled Unclassified Information (CUI) Procedure

1. PURPOSE

This procedure explains the U.S Environmental Protection Agency's (EPA or the Agency) Controlled Unclassified Information (CUI) Program in accordance with Executive Order (E.O.) 13556 and 32 Code of Federal Regulations (CFR) § 2002, both titled "Controlled Unclassified Information." This procedure sets forth standards for the handling, marking, safeguarding, destruction, and decontrolling of CUI for the EPA.

On November 4, 2010, President Obama signed [E.O. 13556, "Controlled Unclassified Information,"](#) establishing the CUI Program and designating the National Archives and Records Administration (NARA) as the CUI Executive Agent (CUI EA) to oversee agency actions and ensure compliance. The Archivist of the United States delegated these responsibilities to the Information Security Oversight Office (ISOO).

The CUI Program is an information security reform designed to establish an open and uniform program for managing unclassified information requiring safeguarding or dissemination controls pursuant to and consistent with laws, regulations, and government-wide policies.

Prior to E.O. 13556, there was a significant need for a uniform method to mark and control unclassified, sensitive information across all Executive Branch agencies. Previously, this information was handled inconsistently because control protocols were developed and implemented at the agency or department level. Under the CUI program established by E.O. 13556, the categories of information listed in the CUI Registry are the exclusive designations for identifying unclassified information that a law, regulation or government-wide policy requires or permits an agency to handle by means of safeguarding or dissemination controls.

On September 14, 2016, NARA issued a final rule amending [32 CFR § 2002](#) to establish a uniform policy for all federal agencies on designating, safeguarding, disseminating, marking, decontrolling, and disposing of CUI; self-inspection and oversight requirements; and other facets of the program.

The CUI Program covers any information that constitutes CUI as defined by 32 CFR § 2002.4(h) and described in section 8 of this procedure ("Definitions").

Directive No: CIO 2158-P-01.1

*Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19*

2. SCOPE

This procedure applies to:

- All CUI, regardless of format, that EPA creates, possesses, receives, or that an entity creates or possesses for or on behalf of EPA, that is required or specifically permitted to be protected under law, regulation, or government-wide policy. All unclassified information throughout EPA and the Executive Branch that requires any CUI safeguarding or dissemination control(s) pursuant to a law, regulation, or government-wide policy is considered CUI. The official list of all CUI categories is found in the U.S. National Archives and Records Administration's (NARA) [CUI Registry](#). Only CUI categories listed on the CUI Registry are authorized for protection as CUI and must be handled consistently with the National CUI Program as defined in EPA Directive CIO 2158.1, Controlled Unclassified Information (CUI) Policy, this procedure, and any subsequent procedures and guidance. CUI shall serve as the exclusive designation for identifying sensitive but unclassified information throughout the Executive Branch, including at EPA. Classified information is not part of this program. Classified information is to be managed in accordance with [E.O. 13526, Classified National Security Information](#) as of December 29, 2009, or the [Atomic Energy Act](#).
- Anyone who handles CUI, including those who handle CUI under arrangements, agreements, contracts, and other transaction authority actions, requiring access to CUI according to terms and conditions including, but not limited to, grants, licenses, certificates, memoranda of agreement/arrangement or understanding, and information-sharing agreements or arrangements (see 32 CFR § 2002.4(c)).

3. AUDIENCE

This procedure applies to all EPA employees, contractors, grantees, and all other users of EPA information and information systems supporting the operations and assets of EPA. This procedure does not apply to entities outside the Agency unless a law, regulation, or government-wide policy requires or permits the controls contained in this procedure to do so, and the CUI Registry lists that law, regulation, or government-wide policy as an authority (32 CFR § 2002.22). This procedure does not apply directly to non-federal entities but does apply indirectly to non-federal recipients of CUI, through incorporation into agreements (32 CFR § 2002.1(f)).

Directive No: CIO 2158-P-01.1

*Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19*

4. AUTHORITY

Procedure CIO 2158-P-01.1 is issued under the authority of EPA Directive CIO 2158.2, Controlled Unclassified Information (CUI) Policy. Additional authorities include:

- [E.O. 13556](#), “Controlled Unclassified Information,” 11/4/2010.
- [32 CFR § 2002](#), “Controlled Unclassified Information,” 9/14/2016.
- [Office of Management and Budget \(OMB\) Circular No. A-11](#), Section 31.15, “Controlled Unclassified Information,” as revised.
- [Federal Information Processing Standards Publication \(FIPS\) Publication \(PUB\) 199](#), “Standards for Security Categorization of Federal Information and Information Systems”, as revised.
- [FIPS PUB 200](#), “Minimum Security Requirements for Federal Information and Information Systems,” as revised.
- [National Institute of Standards and Technology \(NIST\) 800-53, Revision 5](#), “Security and Privacy Controls for Federal Information Systems and Organizations.”
- [NIST 800-88, Revision 1](#), “Guidelines for Media Sanitization.”
- [NIST 800-171, Revision 2](#), “Protecting CUI in Nonfederal Systems and Organizations.”
- [NIST 800-171A](#), “Assessing Security Requirements for CUI.”

5. PROCEDURE

All authorized holders should follow this procedure when marking, safeguarding, and disseminating CUI. Authorized holders are any individual, agency, organization, or group of users that is permitted to designate or handle CUI. Authorized holders of CUI Specified information should follow any this procedure and all requirements of the laws, regulations, or Governmentwide policies on which the CUI Specified designation is based.

In addition to EPA’s CUI Policy and Procedure, additional resources will be available to users:

- Supplemental materials will be provided on the CUI Intranet site, including a marking handbook and user guides; see section 7 of this procedure (“Related Information”).
- Additional guidance on CUI will be published on both EPA’s CUI intranet site and the Agency’s IT/IM Directives website when available.

Directive No: CIO 2158-P-01.1

*Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19*

5.1 Identifying CUI

First, an authorized holder must identify the CUI category or categories for the information. In order to identify CUI, an authorized holder should use the CUI Registry to identify which CUI category (or categories) the information falls into based on the applicable authority or authorities in the CUI Registry. When identifying which CUI category or categories applies to information, the authorized holder should refer to the authorities that are applicable to each category.

[The CUI Registry](#) is the authoritative central repository for all information, guidance, policy, requirements, instructions, and information on CUI, other than E.O. 13556 and 32 CFR § 2002. Only the CUI categories listed in this registry can be used to identify CUI that requires safeguarding or dissemination controls. Personnel may only use those categories published in the CUI Registry to identify information as CUI.

Authorized holders at EPA can reference a list of commonly-used NARA CUI categories posted on the Agency intranet. NARA's CUI Registry is the final authority on CUI categories.

Distinguishing CUI Basic from CUI Specified

There are two types of CUI, CUI Basic and CUI Specified. Whether CUI is CUI Basic or CUI Specified depends on the authority for the CUI. The CUI type for each authority is listed in the CUI Registry. When identifying CUI categories, authorized holders will also need to determine which type of CUI the information is (Basic or Specified) as this will impact the information's marking and safeguarding requirements. For definitions of CUI Basic and CUI Specified see section 8 of this procedure ("Definitions").

5.2 Marking

Second, an authorized holder must mark the information with the appropriate CUI marking.

Apply CUI markings when information is designated as CUI, typically at the time of creation. Information that is under a Legacy Marking Waiver or Limited Marking Waiver does not need to be marked as CUI unless the information will be shared outside of the Agency. For more information on CUI marking waivers, see section 9 of this procedure ("Waivers").

Only apply markings listed in the CUI Registry to designate CUI requiring safeguarding or dissemination controls, unless additional markings are required by an authority. Do not use alternative markings (e.g., FOUO, CBI) to identify or mark information as CUI. You

Directive No: CIO 2158-P-01.1

*Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19*

must handle information in accordance with CUI handling requirements regardless of if the information is marked as CUI. Information may not be marked as CUI for the following purposes:

- To conceal violations of law, inefficiency, or administrative error.
- To prevent embarrassment to the U.S. government, any U.S. official, organization, or agency.
- To improperly or unlawfully interfere with competition.
- To prevent or delay the release of information that does not require such protection.

Authorized holders must adhere to the following requirements in order to properly mark CUI:

Banner Markings

Authorized holders must mark the information as CUI using the banner marking identified in the CUI Registry.

- a. The CUI banner marking must cover all CUI in the document and the CUI banner must be the same on each page. For example, if an authorized holder identifies both legal privilege and privacy information in a document the banner must include markings for both categories on each page.
- b. Banner markings must appear as bold, black and capitalized text at the top of every page, including email transmissions. Banner markings may, depending on the category of CUI, include up to three elements, each of which must be separated by a double forward slash (//):

Note that the banner markings above are the requirements for CUI identified and marked by EPA. Documents received by other agencies may contain slightly different CUI banner markings than required at EPA. The table below spells out the differences between EPA and other agency banner markings.

Directive No: CIO 2158-P-01.1

*Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19*

Category of Marking	EPA CUI Banner Marking Requirements	CUI Received From Other Agencies
CUI Control Marking	<ul style="list-style-type: none"> • Mandatory for all CUI • Should only consist of the acronym "CUI". 	<ul style="list-style-type: none"> • May contain only the word, "CONTROLLED" to indicate the presence of CUI.
CUI Category Marking	<ul style="list-style-type: none"> • Mandatory for all CUI • Applicable category marking must appear in the banner. • For CUI Specified, the category marking must be preceded by a "SP-" (e.g., CUI//SP-PCII). • Multiple categories in the banner must be alphabetized, with CUI Specified categories appearing before any CUI Basic categories. • Multiple categories in a banner line must be separated by a single forward slash (/). 	<ul style="list-style-type: none"> • CUI Basic may or may not include a CUI Category Marking (dependent upon agency policy). • All CUI Specified received will include a CUI Category Marking preceded by a "SP-" (e.g., CUI//SP-PCII).
Limited Dissemination Control Markings (LDCs)	<ul style="list-style-type: none"> • EPA does not permit the use of limited dissemination controls at this time, unless required by an authority. • More information on limited dissemination controls can be found in section 5.4 of this procedure ("Dissemination"). 	<ul style="list-style-type: none"> • May receive CUI banner marking that includes an LDC. • EPA personnel should handle CUI in accordance with any LDCs included in the banner marking. • More information on limited dissemination controls can be found in section 5.4 of this procedure ("Dissemination").

Markings Required by Authority

When marking CUI Specified information, the governing authority may require additional markings or language to be placed on the document. These additional markings may not be placed in or above the CUI banner marking and may not conflict

Directive No: CIO 2158-P-01.1

*Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19*

with portion markings if used. Authorized holders should reference the authority for guidance on how to apply any additional markings. For more information on portion marking, see section 5.2(h) of this procedure (“Portion Marking”).

Designation Indicator

Indicate who designated the information as CUI on all documents containing CUI. This designation indicator must be clearly apparent to authorized holders and may only appear on the first page or cover of a document. When feasible, EPA requires that the “Controlled by” line appears in the center of the footer of the document in black text (e.g., Controlled by the Environmental Protection Agency”).

Decontrolling Indicator (optional)

Where feasible, an authorized holder should include a specific decontrolling date or event on all CUI. This may be accomplished in a manner that makes the decontrolling schedule readily apparent to an authorized holder but must not interfere with the banner marking. For more information on how to decontrol CUI, see section 5.5 of these procedures (“Decontrolling”).

Supplemental Administrative Markings (optional)

Authorized holders must not include supplemental administrative markings (e.g., “Pre-decisional,” “Deliberative,” “Draft”) in the CUI banner marking, nor may they be incorporated into the CUI designating/decontrolling indicators or portion markings but may be included elsewhere on the document such as in a watermark. Supplemental administrative markings may not impose additional safeguarding requirements or disseminating restrictions or designate the information as CUI. Their purpose is to inform recipients of the status of documents under development to avoid confusion and maintain the integrity of a decision-making process. Supplemental markings, other than the universally accepted “DRAFT,” shall, on the first page or the first time it appears, include an explanation or intent of the marking (e.g., Pre-decisional – “The information in this document provides background, options, and/or recommendations about safeguarding CUI data.”).

Alternative Marking Methods

When it is impractical to individually mark CUI due to quantity or nature of the information, or when the EPA has issued a limited CUI marking waiver, authorized holders must make recipients aware of the information’s CUI status using an alternate marking method that is readily apparent. This could be done through methods such as user access agreements, computer system digital splash screens, or signs in storage areas or in containers.

Directive No: CIO 2158-P-01.1

*Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19*

Legacy Markings

Markings which were applied prior to the start of the CUI Program, and are inconsistent with the CUI markings, are considered legacy markings (e.g., For Official Use Only, Agency Internal Use Only). Information with legacy markings that is not shared outside of the Agency does not need to be remarked with CUI markings. However, if an authorized holder is using legacy information or information derived from a legacy document that qualifies as CUI in a new document, the new document must contain CUI markings and follow proper safeguarding and handling guidelines. A Legacy Marking Waiver is in place for information created prior to the CUI implementation date. For more information on exceptions to this rule, see section 9 of this procedure (“Waivers”).

Commingling CUI Markings: Classified National Security Information (CNSI)

When authorized holders include CUI in documents that also contain CNSI, personnel must:

- Portion mark all CUI to ensure that authorized holders can distinguish CUI portions from portions containing classified and uncontrolled unclassified information; and
- Include the CUI control marking, CUI Specified category markings, and any limited dissemination control markings in the overall banner marking.

Portion Markings (permitted only for CUI commingled with CNSI information)

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

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. Sections that do not contain CUI should be marked as Uncontrolled Unclassified Information, designated with a [U].

In commingled documents, decontrolling provisions of the CUI Program apply only to portions marked as CUI. The EPA Marking Handbook will contain specific guidance on marking CUI when commingled with CNSI.

Commingling CUI Markings: Restricted Data (RD) and Formerly Restricted Data (FRD)

To the extent possible, avoid commingling RD or FRD with CUI in the same document. When it is not practical to avoid such commingling, follow the marking requirements in E.O. 13556, 32 CFR § 2002, and in the instructions in the CUI Registry, as well as the marking requirements in 10 CFR § 1045, “Nuclear Classification and Declassification.”

Directive No: CIO 2158-P-01.1

*Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19*

Packages and Parcels

Packages or parcels containing CUI must be addressed for delivery only to a specific recipient. Do not put CUI markings on the outside of an envelope or package, or otherwise indicate on the outside that the item contains CUI. For more information on mailing CUI, see section 5.4 of these procedures (“Dissemination”).

Transmittal Markings

When a transmittal document accompanies CUI (e.g., fax cover sheet), the transmittal document must include a CUI control marking (i.e., “CUI”) on its face, indicating that CUI is attached or enclosed. Additionally, the transmittal document must include conspicuously on its face the following or similar instructions, as appropriate:

- “When enclosure is removed, this document is Uncontrolled Unclassified Information”; or
- “When enclosure is removed, this document is (control level); upon removal, this document does not contain CUI.”

Working Papers

Mark working papers containing CUI the same way as the finished product containing CUI would be marked.

5.3 Safeguarding

Third, an authorized holder must properly handle and safeguard CUI. Safeguarding standards (i.e., CUI Basic and CUI Specified controls) are issued by the CUI EA in both 32 CFR § 2002 and in the CUI Registry and are updated as needed.

Safeguarding CUI Specified

- Authorized holders must protect CUI Specified in accordance with the requirements of the underlying authorities indicated in the CUI Registry.
- When the laws, regulations, or Government-wide policies governing a specific type of CUI Specified are silent on either a safeguarding or disseminating control, authorized holders must protect the information with CUI Basic requirements, unless this results in treatment that does not accord with the CUI Specified authority.

Safeguarding CUI Basic

- Authorized holders must protect CUI Basic in accordance with the following requirements as identified in 32 CFR § 2002.
- Authorized holders may not require additional controls for CUI Basic at a level higher these requirements when disseminating CUI Basic outside the Agency.

Directive No: CIO 2158-P-01.1

*Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19*

Controlled Environments

Authorized holders must establish controlled environments to protect CUI from unauthorized access or disclosure. A controlled environment is any area or space that an authorized holder deems to have adequate physical or procedural controls (e.g., barriers and managed access controls) to protect CUI from unauthorized access or disclosure. If CUI is not in a controlled environment, authorized holders must reasonably ensure that unauthorized individuals cannot access or observe CUI or overhear conversations in which CUI is discussed. This must be done by keeping CUI under the authorized holder's direct control or protected with at least one physical barrier. Unless different protection is specified in the CUI Registry, CUI must be stored in a locked office, locked drawer, or locked file cabinet whenever it is left unattended.

Teleworking with CUI

Authorized holders must ensure that CUI is always protected with one physical barrier if handled while teleworking. For example, authorized users should only access CUI from a secure location, such as a home office, where unauthorized holders cannot observe.

Cover Sheets

Authorized holders may use cover sheets to identify CUI, alert observers that CUI is present from a distance, and to serve as a shield to protect the attached CUI from inadvertent disclosure. Cover sheet use is optional but if a CUI coversheet is needed, the authorized holder must use the NARA-approved cover sheet, [Standard Form \(SF\) 901](#).

Safeguarding Electronic Systems

Information systems that process, store, or transmit CUI must be safeguarded in accordance with FIPS PUB 199, where CUI Basic is categorized at no less than the moderate confidentiality impact level. FIPS PUB 199 defines the security impact levels for federal information in both federal and non-federal information systems. If unsure whether an information system is appropriately secure for storing CUI, authorized holders should seek confirmation from the appropriate Information Security Officer.

1. **Federal Information Systems**

The appropriate security requirements and controls identified in FIPS PUB 200 and NIST SP 800-53 must be applied to CUI in accordance with any risk-based tailoring decisions made. EPA may increase CUI Basic's confidentiality impact level above moderate only within EPA, including contractors operating an information system on behalf of EPA, or by means of agreements between EPA and other agencies. EPA may not otherwise require controls for CUI Basic at a level higher or different from those permitted in the CUI Basic requirements when disseminating the CUI Basic outside EPA.

Directive No: CIO 2158-P-01.1

*Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19*

2. **Non-Federal Information Systems**

NIST Special Publication 800-171 contains standards that EPA contractors must meet if they have EPA CUI on their computer systems.

Systems authorized to store, process, and/or transmit classified information are considered sufficient for the protection of CUI provided that access, dissemination, and marking protections are adhered to including all National Security Systems (even those not approved for classified information).

Destruction

Authorized holders may destroy CUI when the information is no longer needed, and when records disposition schedules, published or approved by NARA or other applicable laws, regulations, or government-wide policies, no longer require retention.

Destruction of CUI, including in electronic form, must be accomplished in a manner that makes it unreadable, indecipherable, and irrecoverable. CUI may not be placed in office trash bins or recycling containers. CUI Specified must be destroyed according to any specific directives regarding the information. Guidance for destruction in NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, and NIST SP 800-88, Guidelines for Media Sanitization (incorporated by reference, see § 2002.2); or any method of destruction approved for Classified National Security Information, as delineated in 32 CFR 2001.47, Destruction, or any implementing or successor guidance.

5.4 Dissemination

Fourth, authorized holders should disseminate and permit access to CUI, provided that such access or dissemination:

- Abides by the laws, regulations, or government-wide policies that established the CUI category;
- Furthers a lawful government purpose;
- Is not restricted by an authorized limited dissemination control established by the CUI EA; and
- Is not otherwise prohibited by law.

When sharing CUI, authorized holders must reasonably expect that all intended recipients are authorized to receive the CUI, have a basic understanding of how to handle it, and have a lawful government purpose to receive the CUI. When determining whether CUI may be shared, a reasonable expectation does not supersede relevant

Directive No: CIO 2158-P-01.1

*Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19*

statutory or regulatory requirements. Staff should continue to follow any dissemination requirements, as defined in the underlying authority for that information.

CUI Basic may be disseminated to persons and entities who have a lawful government purpose to access the information.

CUI Specified may only be disseminated to persons and entities as authorized in the underlying legislation or authority contained in the CUI Registry. Further dissemination of CUI Specified may be made to such authorized persons if not restricted by the underlying authority (governing law, regulation, or government-wide policy).

Limited Dissemination Controls

Only the limited dissemination controls published in the CUI Registry may be used to restrict the dissemination of CUI to certain individuals, agencies, or organizations. These dissemination controls may only be used to further a lawful government purpose, or if laws, regulations, or government-wide policies require or permit their use.

At this time EPA does not permit the use of limited dissemination controls, unless required by an authority. If at any point EPA allows the use of limited dissemination controls, approved limited dissemination controls will be located in the EPA CUI Marking Handbook. Authorized holders should continue to handle CUI with existing limited dissemination controls designated by other federal agencies accordingly.

Sharing with a Non-Executive Branch or Foreign Entity

Authorized holders may share CUI with a non-federal or a foreign entity as long as both the dissemination requirements listed above and the following conditions are met:

- When there is a reasonable expectation that all intended recipients are authorized to receive the CUI and have a basic understanding of how to handle it; and
- Whenever feasible, the Region or Program Office shall enter into some type of formal information-sharing agreement with the recipient of the CUI. The agreement must include a requirement for the recipient to, at a minimum, comply with EO 13556; 32 CFR Part 2002; and the CUI Registry.

When entering into information-sharing agreements or arrangements with a foreign entity, personnel should encourage that entity to protect CUI in accordance with EO 13556; 32 CFR Part 2002; and the CUI Registry. Personnel are cautioned to use judgment as to what and how much to communicate, keeping in mind the ultimate goal of safeguarding CUI. If such agreements or arrangements include safeguarding or dissemination controls on unclassified information, only the CUI markings and controls may be allowed. Other markings or protective measures may not be used.

Directive No: CIO 2158-P-01.1

*Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19*

Information-Sharing Agreements

Information-sharing agreements that were made prior to establishment of the CUI Program should be modified whenever feasible so they do not conflict with CUI Program requirements. [§ 2002.16(a)(5)(iv)]

Information-sharing agreements with non-federal entities must include provisions that CUI be handled in accordance with the CUI Program; misuse of CUI is subject to penalties established in applicable laws, regulations, or government-wide policies; and any non-compliance with handling requirements must be reported to the CUI SAO. When the EPA is not the designating agency, personnel must report any non-compliance to the designating agency. [§ 2002.16(a)(6)]

Mailing CUI

Before mailing CUI, the authorized holder must ensure that the recipient is an authorized holder of the information and can properly handle and safeguard it. Below are some of the methods that may be used to deliver CUI:

Method	Recipient	Requirements
Interoffice or interagency mail systems	May be used to transport CUI internally	Sender must ensure that all markings are properly displayed on the documents before delivery
The United States Postal Service, UPS, FedEx, or any other commercial delivery service	May be used to transport or deliver CUI to another entity	CUI sent via these channels must: <ul style="list-style-type: none"> • Have in-transit automated tracking and accountability tools • Envelopes or packages that contain CUI should indicate that they are intended for the addressed recipient only and must not be forwarded • No CUI markings should be placed on the outside of an envelope or package
Hand delivery	May be used to transport CUI internally	Sender must ensure that all markings are properly displayed on the documents before delivery

Directive No: CIO 2158-P-01.1

*Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19*

Printing, Faxing, or Scanning CUI

Authorized holders may reproduce CUI (i.e., copied, scanned, printed) in furtherance of a lawful government purpose and only using government furnished equipment (GFE). When reproducing CUI documents on equipment such as printers, copiers, scanners, or fax machines, system owners must ensure that the equipment does not retain data or transmit the data to a non-federal entity, or else they must sanitize it in accordance with NIST SP 800-53. Prior to purchasing equipment, management should ensure that it does not store or transmit data to non-federal entities and that at the end of the equipment's lifecycle any hard drives or memory is sanitized in accordance with NIST SP 800-88.

5.5 Decontrolling

CUI may be decontrolled when it no longer requires safeguarding or dissemination controls, unless doing so conflicts with the governing law, regulation, or government-wide policy. Only the designating agency may decontrol the CUI.

5.6 Misuse of CUI

Misuse of CUI may result in administrative or disciplinary action, up to and including removal from federal service. Some misuses of CUI may also result in criminal penalties as outlined in the underlying law, regulation, or government-wide policy governing protection of the information. Any disciplinary action shall be guided by E.O. 9830, as amended, and Chapters 43 and 75 of Title 5 of the U.S. Code. In the event a contractor misuses CUI, the matter must be referred to the CO to determine whether remedies should be imposed under the contract. Follow incident response procedures for any misuse of CUI (EPA Directive CIO 2150-P-08.2, Information Security – Incident Response Procedures).

5.7 Training

All managers, supervisors, employees, and contractors will receive mandatory training annually. New employees and contractors must receive initial training within 180 days of beginning employment.

5.8 Self-Inspection

In accordance with 32 CFR § 2002.8(b)(4), the EPA CUI Program will implement a Self-Inspection Program that includes:

- At a minimum, an annual review and assessment of the Agency's CUI program. The Agency head or CUI SAO should determine any greater frequency based on program needs and the degree to which the Agency engages in designating CUI;

Directive No: CIO 2158-P-01.1

*Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19*

- Self-inspection methods, reviews, and assessments that serve to evaluate program effectiveness, measure the level of compliance, and monitor the progress of CUI implementation;
- Formats for documenting self-inspections and recording findings when not prescribed by the CUI EA;
- 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; and
- Analysis and conclusions from the self-inspection program, documented on an annual basis and as requested by the CUI EA.

5.9 CUI and Disclosure Statutes

CUI does not override the requirements of existing disclosure statutes. Disclosure determinations must be based on the applicable law, regulation, or government-wide policy and not the information's status as CUI.

CUI and the Freedom of Information Act (FOIA)

EPA Offices and Regions must not cite the Freedom of Information Act (FOIA) as a CUI safeguarding or disseminating control authority for CUI. The CUI procedures do not alter or eliminate any aspect of EPA's FOIA regulations, policy, or procedures. When determining whether to disclose information in response to a FOIA request, the decision must be based on the content of the information and applicability of any FOIA statutory exemptions, regardless of whether an agency designates or marks the information as CUI. In circumstances where CUI is disclosed to an individual or entity through a FOIA response, this does not automatically constitute public release as defined in 32 CFR § 2002. Authorized holders still need to control the CUI while the agency continues to hold the information, despite the disclosure, unless the information has been formally decontrolled in accordance with CUI policy and procedure.

If an EPA Office or Region determines that, despite public disclosure of the CUI through FOIA, there is still an identifiable need to continue to protect the information as CUI within the Agency, then the EPA Office or Region must consult with the appropriate legal office (i.e., Office of General Counsel/General Law Office or Office of Regional Counsel).

CUI and the Whistleblower Protection Act

The CUI Program does not change or affect existing legal protections for whistleblowers. The fact that information is marked or designated as CUI does not determine whether an individual may lawfully disclose that information under a law or other authority and

Directive No: CIO 2158-P-01.1

*Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19*

does not preempt or otherwise affect whistleblower legal protections provided by law, regulation, or executive order or directive.

CUI and the Administrative Procedure Act

The CUI Program does not alter the Administrative Procedure Act (APA), or the powers of Federal administrative law judges (ALJs) appointed thereunder, including the power to determine confidentiality of information in proceedings over which they preside. Nor do CUI regulations impose requirements concerning the way ALJs designate, disseminate, control access to, decontrol, or mark such information, or make such determinations.

CUI and the Privacy Act

EPA personnel should manage records in accordance with the Privacy Act of 1974 regardless of any CUI markings.

The fact that records are subject to the Privacy Act of 1974 does not mean that agencies must mark them as CUI. Authorized holders should consult Agency policies or guidance to determine which records may be subject to the Privacy Act; and the CUI Registry to determine which privacy information must be marked as CUI. Information contained in Privacy Act systems of records may also be subject to controls under other CUI categories and the Agency may need to mark that information as CUI for that reason. In addition, when determining whether the Agency must protect certain information under the Privacy Act, or whether the Privacy Act allows the Agency to release the information to an individual, the Agency must base its decision on the content of the information and the Privacy Act's criteria, regardless of whether an Agency designates or marks the information as CUI.

6. ROLES AND RESPONSIBILITIES

The EPA Administrator has the authority to approve the establishment of an EPA CUI Program. The EPA Administrator has delegated this authority to the CIO, in the Office of Mission Support (OMS). The following roles are the core of the CUI Program. As necessary, subsequent procedures will further refine these roles and responsibilities.

EPA Chief Information Officer (CIO):

- a) Ensures senior leadership support and adequate resources are available for implementation, management, and oversight of the CUI Program.
- b) Issues and promulgates CUI policy and procedures to ensure that EPA complies with all CUI requirements in accordance with 32 CFR § 2002.
- c) Ensures EPA's strategic plans include CUI compliance requirements.

Directive No: CIO 2158-P-01.1

*Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19*

- d) Ensures enforcement and compliance with CUI and related information directives.
- e) Ensures that CUI management processes are integrated with Agency strategic and operational planning processes.
- f) Designates the EPA Senior Agency Official for Controlled Unclassified Information (SAO for CUI) in writing. EPA SAO for CUI must be at the Senior Executive Service (SES) level or equivalent.
- g) Oversees the activities of the EPA SAO for CUI.
- h) Reviews and approves CUI annual reports to the CUI Executive Agent created by the EPA CUI PM.

EPA Senior Agency Official for Controlled Unclassified Information (SAO for CUI):

- a) Designated by the EPA CIO.
- b) Holds overarching responsibility for the CUI Program within EPA. The EPA CIO has designated the Office of Records, Administrative Systems and eDiscovery (ORASE) Director as the SAO for CUI responsible for EPA's CUI Program.
- c) Directs and oversees EPA's CUI Program in accordance with 32 CFR § 2002.8 and delegates responsibilities to the EPA CUI PM as needed.
- d) Ensures the Agency establishes policies and plans needed to implement CUI.
- e) Ensures EPA's CUI compliance with laws, regulations, and EPA policy in collaboration with the EPA Chief Information Security Officer (CISO) and EPA Senior Agency Official for Privacy (SAOP).
- f) Ensures the position of the EPA PM is never vacant and notifies the CUI Executive Agent when the individual serving as the EPA CUI PM changes.
- g) Reviews and approves CUI annual reports to the CUI Executive Agent created by the CUI PM.

EPA CUI Program Manager (PM):

- a) Designated by the EPA SAO for CUI.
- b) Coordinates all aspects of the day-to-day activities of the EPA CUI Program, supported by CUI Liaisons from Program Offices and Regions with CUI responsibilities.
- c) Chairs the EPA's CUI Advisory Committee (CUIAC) with CUI Liaison representatives from every Program Office and Region.
- d) Develops Agency-level CUI policy, procedures, standards, and guidelines.
- e) Develops a CUI education and training program and ensures all Agency personnel, including contractors and other affiliates, receive appropriate CUI Training.
- f) Provides overall CUI management and policy guidance.
- g) Develops and implements EPA's self-inspection program.
- h) Establishes a process to accept and manage challenges to CUI statutes (e.g., improper or absence of marking), based on laws, regulations, and government-wide policies.

Directive No: CIO 2158-P-01.1

*Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19*

- i) Submits official CUI annual reports to the CUI Executive Agent on behalf of the SAO for CUI.
- j) Represents EPA at government-wide NARA meetings (e.g., CUI Advisory Council, CUI Registry Committee).
- k) Submits to the CUI Executive Agent any law, regulation, or government-wide policy not already incorporated in the CUI Registry that EPA proposes to use to designate unclassified information for safeguarding or dissemination controls.
- l) Coordinates with the CUI Executive Agent, as appropriate, on any proposed law, regulation, or government-wide policy that would establish, eliminate, or modify a category of CUI, or change information controls applicable to CUI.
- m) Coordinates with the CISO to ensure that Privacy and Security policy, procedures, and guidance are consistent with respect to safeguarding CUI.
- n) Provides all existing waivers in the annual report to the CUI Executive Agent, along with the rationale for each waiver and, where applicable, the alternative steps EPA is taking to ensure sufficient protection of CUI within the Agency.
- o) Establishes processes for handling CUI decontrol requests.
- p) Establishes processes and procedures for authorized holders (both inside and outside EPA) to be able to contact a designated agency representative for instructions upon receiving unmarked or improperly marked information that the agency has designated as CUI.
- q) Communicates CUI Program updates to Program Offices and Regions, as needed.
- r) Performs delegated responsibilities from the SAO for CUI as needed.

EPA Chief Information Security Officer (CISO):

- a) Ensures that EPA's information systems that process, transmit, or store CUI are at the *Federal Information Security Modernization Act of 2014* (FISMA) confidentiality impact level of Moderate.
- b) Ensures that the CUI incident, misuse, or data leak response is incorporated in EPA's Computer Security Incident Response Center (CSIRC) processes.

Senior Information Officials (SIO):

- a) Responsible for ensuring compliance with this CUI policy and subsequent procedures, standards and guidelines.
- b) Designate a primary and alternate CUI Liaison and ensure these positions are never vacant. These positions will work with the EPA CUI PM and SAO for CUI on implementation and oversight of CUI.
- c) Ensures CUI is part of the IT Portfolio Review to validate that all information systems processing, transmitting, or storing CUI are raised to meet the FISMA confidentiality impact level of Moderate.
- d) Ensures any costs associated with needed information system upgrades/changes are budgeted and planned for within 180 days after this policy becomes effective.

Directive No: CIO 2158-P-01.1

*Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19*

- e) Ensures all information systems under their purview are marked in compliance with CUI policy.

CUI Liaisons:

- a) Primary and alternate are designated by the SIO of their respective Regions or Program Offices.
- b) Serve as a CUI point of contact and subject matter expert to their respective Regions or Program Offices.
- c) Solicit input from their respective Regions or Program Offices to engage stakeholders for the purposes of implementation.
- d) Assist in the communication of all CUI updates to their respective Regions or Program Offices.
- e) Attend monthly Committee meetings or designate a proxy in the event neither the primary nor the alternate are able to attend.

EPA CUI Advisory Committee (CUIAC):

- a) Chaired by the EPA CUI PM.
- b) Members consist of the EPA SAO for CUI, a primary and alternate CUI Liaison from each Region and Program Office, subject matter experts as appropriate, and any CUI support staff.
- c) Members advise and assist the EPA CUI PM and SAO for CUI in developing and implementing the Agency's CUI goals and policies, including subsequent procedures, standards, and guidelines.
- d) Members serve as the Agency's CUI governance body to advise and assist on matters affecting the Regions and Program Offices.
- e) Members review and provide feedback on all CUI-related matters as the official representatives of their respective Region or Program Office of origin.

Contracting Officers (CO) and Contracting Officer Representatives (COR):

- a) Ensure that the appropriate requirements of this policy are included in all procurement actions that relate to CUI.
- b) Ensure that the FAR clause and accompanying CUI Standard Form (SF) on CUI are incorporated in current and future contracts once the clause is finalized.

Supervisors and Managers:

- a) Ensure staff adherence to all CUI policy and procedures. This includes ensuring policies, procedures, standards, guidelines, training, etc., are examined and, if needed, are modified to include or reference CUI Program requirements.
- b) Annually verify that all physical safeguarding measures for individual workspaces are adequate for the protection of CUI (i.e., prevent unauthorized access) and ensure that all personnel under their purview receive CUI training as required by this policy.

Directive No: CIO 2158-P-01.1

*Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19*

All EPA employees, contractors, and other affiliates:

- a) Mark, safeguard, and appropriately disseminate CUI when encountering and handling it.
- b) Take the mandatory CUI training within 180 days of beginning employment and on an annual basis.
- c) Immediately report any misuse of CUI, including unmarked or improperly marked CUI, in accordance with the Agency's incident response procedures (EPA Directive CIO 2150-P-08.2, Information Security – Incident Response Procedures).

Agency Records Officers:

- a) Oversee EPA's National Records Management Program and provide guidance and oversight on recordkeeping responsibilities.
- b) Ensure records management policies, procedures, training, etc., address the transferring of EPA Records to NARA.
- c) Ensure EPA's records management guidance reflects CUI requirements.

7. RELATED INFORMATION

- [CUI Notices and Executive Agent Guidance](#)
- [E.O. 13556 Overview](#) for Departments and Agencies
- [Information Security Policy](#) (CIO 2150.6)
- [Records Management Policy](#) (CIO 2155.5)
- [Information Security – Incident Response Procedures](#) (CIO 2150-P-08.2)
- [Office of Management and Budget \(OMB\) Circular No. A-11](#), Section 31.15, "Controlled Unclassified Information," as revised.
- [Federal Information Processing Standards Publication \(FIPS\) Publication \(PUB\) 199](#), "Standards for Security Categorization of Federal Information and Information Systems", as revised.
- [FIPS PUB 200](#), "Minimum Security Requirements for Federal Information and Information Systems," as revised.
- [National Institute of Standards and Technology \(NIST\) 800-53, Revision 5](#), "Security and Privacy Controls for Federal Information Systems and Organizations."
- [NIST 800-88, Revision 1](#), "Guidelines for Media Sanitization."
- [NIST 800-171, Revision 2](#), "Protecting CUI in Nonfederal Systems and Organizations."
- [NIST 800-171A](#), "Assessing Security Requirements for CUI."
- [Privacy Policy](#) (CIO 2151.1)
- [EPA CUI Intranet site](#)

8. DEFINITIONS

Agreements and arrangements are any vehicle that sets up specific CUI handling requirements for contractors and other information-sharing partners when the arrangement with the other partner involves CUI. Agreements and arrangements include, but are not limited to, contracts, grants, licenses, certificates, memoranda of agreement/arrangement or understanding, and information sharing agreements or arrangements. When disseminating or sharing CUI with non-federal entities, including foreign entities, agencies should enter into agreements or arrangements when feasible.

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

Challenges occur when authorized holders believe, in good faith, that a designation of CUI is improper or incorrect, or believe that they have received unmarked CUI, and thus notify the designating agency of this belief. Challenges may be made anonymously; and challengers cannot be subject to retribution for bringing such challenges to light.

Classified Information is information that has been determined pursuant to EO 13526, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended, to require agencies to mark with classified markings and protect against unauthorized disclosure.

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

Control level is a general term that indicates the safeguarding and dissemination requirements associated with CUI Basic and CUI Specified.

CUI is information the government creates or possesses, or that an entity creates or possesses for or on behalf of the government, that a law, regulation, or government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. CUI does not include classified information or information a non-federal entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, a federal agency or an entity acting for an agency.

CUI Basic is the subset of CUI for which the authorizing law, regulation, or government-wide policy does not set out specific handling or dissemination controls. Agencies handle CUI Basic according to the uniform set of controls set forth in 32 CFR § Part 2002

Directive No: CIO 2158-P-01.1

*Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19*

and the CUI Registry. CUI Basic differs from CUI Specified (see definition for CUI Specified), and CUI Basic controls apply whenever CUI Specified ones do not cover the involved CUI.

CUI Categories are types of information for which the law, regulation, or government-wide policy require or permit agencies to exercise safeguarding or dissemination controls, and which the CUI Executive Agent (EA) has approved and listed in the CUI Registry.

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

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

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, which differ from those for CUI Basic. 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 specific controls for CUI Specified information and does not for CUI Basic information.

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

Designating CUI occurs when an authorized holder, consistent with 32 CFR § 2002 and the CUI Registry, determines that a specific item of information falls into a CUI category.

Designation Agency is the federal agency that designates or approves the designation of a specific item of information as CUI.

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

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

Federal information system is an information system used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. An information system operated on behalf of an agency provides information 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). Information systems that a non-federal entity operates on behalf of an agency are subject to the requirements of 32 CFR part § Part 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. An information system used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.

Directive No: CIO 2158-P-01.1

*Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19*

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

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

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

Incident refers to an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality or availability of information or an information system or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

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

Legacy markings are markings applied prior to the start of the CUI Program on unclassified information that requires access or dissemination controls (e.g., For Official Use Only).

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

Misuse of CUI occurs when someone uses CUI in a manner not in accordance with the policy contained in E.O. 13556, 32 CFR § Part 2002, the CUI Registry, agency CUI policy, or the applicable law, regulation, or government-wide policy 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.

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

Directive No: CIO 2158-P-01.1

*Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19*

federal disclosure laws, including the Freedom of Information Act (FOIA) 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-federal entities protect these systems in the same manner that the agencies might protect their own information systems. When a non-federal 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.

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

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

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

Public release occurs when the agency that originally designated information as CUI makes that information available to the public through the agency's official public release processes. Disseminating CUI to non-federal entities as authorized does not constitute public release. Releasing information to an individual pursuant to the Privacy Act of 1974 or disclosing it in response to a Freedom of Information Act (FOIA) request also does not automatically constitute public release, although it may if that agency ties such actions to its official public release processes. Even though an agency may disclose some CUI to a member of the public, the government must still control that CUI unless the agency publicly releases it through its official public release processes.

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

Required or permitted (by a law, regulation, or government-wide policy) is the basis by which information may qualify as CUI. If a law, regulation, or government-wide policy

Directive No: CIO 2158-P-01.1

*Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19*

requires that agencies exercise safeguarding or dissemination controls over certain information, or specifically permits agencies the discretion to do so, then that information qualifies as CUI. The term “specifically permits” in this context can include language such as “is exempt from” applying certain information release or disclosure requirements, “may” release or disclose the information, “may not be required to” release or disclose the information, “is responsible for protecting” the information, and similar specific but indirect, forms of granting the agency discretion regarding safeguarding or dissemination controls. This does not include general agency or agency head authority and discretion to make decisions, risk assessments, or other broad agency authorities, discretions, and powers, regardless of the source. The CUI Registry reflects all appropriate authorizing authorities.

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

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

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

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

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

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

9. WAIVERS

The EPA SAO for CUI may approve waivers of all or some of the CUI marking requirements while the CUI remains within EPA, if it is determined that, due to a substantial amount of stored information with legacy markings, removing legacy markings or re-marking it as CUI would be excessively burdensome unless specifically

Directive No: CIO 2158-P-01.1

*Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19*

prohibited by applicable laws, regulations, or government-wide policies. CUI Waivers approved by the EPA CUI SAO will be located on both EPA's CUI internet and intranet sites.

9.1 Waiver Requirements

All authorized holders of CUI shall:

- Safeguard all CUI under a Marking Waiver in accordance with 32 CFR § 2002 and any existing authority (law, regulation, or government wide policy). For more information, see section 5.3 of these procedures ("Safeguarding").
- When re-using any legacy information or information derived from legacy documents that qualifies as CUI, will redact legacy markings and designate or re-mark the information as CUI, even if the information is under a legacy material marking waiver prior to re-use.
- Apply CUI markings uniformly and conspicuously to all CUI prior to disseminating it outside the EPA unless otherwise specifically permitted by NARA. Waivers approved by the CUI SAO are valid only while the information remains within the EPA.

The CUI PM shall:

- Retain a record of each waiver.
- Include a description of all current waivers and waivers issued during the preceding year in the annual report to NARA, along with the rationale for each waiver and the alternate steps the agency takes to ensure sufficient protection of CUI.
- Notify authorized recipients and the public of these waivers through means such as notices or websites.

Exigent Circumstances

- In exigent circumstances,¹ the CUI SAO may waive certain requirements of the CUI Program for any CUI while it is within the EPA's possession or control, unless specifically prohibited by applicable laws, regulations, or government-wide policies.
- Exigent circumstances waivers may apply when the EPA shares the information with other agencies or non-federal entities. In such cases, recipients must be made aware of the CUI status of any disseminated information.

¹ *Exigent circumstances exist when following proper procedures would cause an unacceptable delay due to the urgency of the situation.*

Directive No: CIO 2158-P-01.1

*Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19*

9.2 Agency Waivers

Legacy Marking Waiver

A Legacy Marking Waiver is in place for information created prior to the CUI implementation date. Legacy information that is not shared outside of the Agency does not need to be remarked with CUI markings. However, if an authorized holder is using legacy information or information derived from a legacy document that qualifies as CUI in a new document, the new document must contain CUI markings and follow proper safeguarding and handling guidelines.

Limited Marking Waivers

The only authorized Limited Marking Waivers are the ones reviewed, approved, and implemented at EPA on a case-by-case basis where it has been determined that marking the information as CUI is excessively burdensome. All approved Limited Marking Waivers can be found on both the Agency's public internet and internal intranet sites.

10. DIRECTIVE(S) SUPERSEDED

Controlled Unclassified Information (CUI) Procedure, CIO 2158-P-01.0, January 2023.

11. CONTACTS

For additional information about this policy, please contact the Office of Mission Support (OMS), Office of Records, Administrative Systems, and eDiscovery (ORASE), Enterprise Records Management and CUI Division (ERMCD).

***Vaughn Noga, Chief Information Officer and Deputy Assistant Administrator
for Information Technology and Information Management***