Description of document:	Department of the Treasury Directive Publication 80-08: Controlled Unclassified Information (CUI) Guide, 2018
Requested date:	28-June-2021
Release date:	12-July-2021
Posted date:	10-January-2022
Source of document:	FOIA and Transparency FOIA Request Department of the Treasury Washington, DC 20220 Fax: 202-622-3895 Email: FOIA@treasury.gov FOIA.gov

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

7/12/2021

RE: Your FOIA Request to Treasury, Case Number 2021-FOIA-00701

This is the final response of the Department of the Treasury (Treasury) to your Freedom of Information Act (FOIA) request dated 6/28/2021. You have requested access to the following records:

"A copy of the Dept of the Treasury CUI Policy document. CUI stands for Controlled Unclassified Information. This document was completed circa 2020."

Your request has been processed under the provisions of the FOIA, 5 U.S.C. § 552. A reasonable search was conducted for records responsive to your request. In response to the search, 28 pages were located within the Departmental Offices of Treasury. After review, I have determined that the records will be released to you in their entirety. No exemptions have been claimed. Additional information of potential interest can be located at https://home.treasury.gov/about/general-information/orders-and-directives/td80-08.

There are no fees assessed at this time since allowable charges fell below $25.

You may reach us via telephone at 202-622-0930, extension 2; or via e-mail at FOIA@treasury.gov. Please reference FOIA case number 2021-FOIA-00701 when contacting our office about this request.

Sincerely,

Mark Bittner
Director, FOIA & Transparency
Office of Privacy, Transparency, and Records

Enclosures
Responsive document set (28 pages)

TREASURY DIRECTIVE PUBLICATION 80-08

Controlled Unclassified Information (CUI)

Guide

09/04/2018

CONTROLLED
UNCLASSIFIED
INFORMATION

TABLE OF CONTENTS

Treasury Directive Publication (TD P 80-08)

Controlled Unclassified Information (CUI) Guide

This TD P provides further directions to all bureaus, offices, and organizations in the Department of the Treasury for compliance with TD 80-08.

1. INTRODUCTION

In November 2010, the President issued Executive Order (EO) 13556, *Controlled Unclassified Information* (CUI), to "establish an open and uniform program for managing [unclassified] information that requires safeguarding or dissemination controls." Prior to that time, more than 100 different markings for such information existed across the executive branch. This *ad hoc*, agency-specific approach created inefficiency and confusion, led to a patchwork system that failed to adequately safeguard information requiring protection, and unnecessarily restricted information-sharing.

EO 13556 established the CUI Program to standardize and simplify the way the executive branch handles unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with applicable laws, regulations, and government-wide policies.

The National Archives and Records Administration (NARA) is the CUI Executive Agent responsible for developing policy and providing oversight for the CUI Program.

NARA established a CUI Registry[1] on its website that serves as the authoritative reference for all CUI categories, subcategories, and markings.

2. PURPOSE

This TD P implements EO 13556 and 32 CFR Part 2002, both entitled *Controlled Unclassified Information*. These directives institute national policy on the handling, safeguarding, and control of 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. Classified information is not part of the CUI Program; EO 13526 applies to Classified National Security Information.

3. AUTHORITY

TD P 80-08 is issued under the authority of Treasury Directive (TD) 80-08, *Controlled Unclassified Information (CUI) Policy*, dated October 19, 2017.

4. APPLICABILITY

[1] The CUI Registry can be located at www.archives.gov/cui

This TD P sets forth policy for the handling, marking, protecting, destroying, and decontrolling of CUI for Departmental Offices (DO), Treasury bureaus, and the Offices of Inspectors General (collectively bureaus). This TD P applies to all personnel, including employees, contractor employees, detailees, and interns, who may come in contact with CUI in the performance of official Treasury duties.

The provisions of this TD P shall not be construed to interfere with or impede the authorities or independence of the Treasury Inspector General, the Treasury Inspector General for Tax Administration, or the Special Inspector General for the Troubled Asset Relief Program.

5. LIMITATIONS ON APPLICABILITY OF THIS TD P [§ 2002.22]

Any CUI requirements contained within this TD P or Treasury bureau policies that are not supported by law, regulation, or government-wide policy may not be applied to outside entities. When entering into agreements, Treasury organizations may not include additional requirements or restrictions on handling CUI other than those permitted in the CUI Program.

6. REFERENCES[2]

EO 13556, *Controlled Unclassified Information*, November 4, 2010

32 CFR Part 2002, *Controlled Unclassified Information*, September 14, 2016

National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004

NIST FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006

NIST Special Publication (SP) 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013 (updated 01-22-2015)

NIST SP 800-88, Revision 1, Guidelines for Media Sanitization, December 2014

NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, Revision 1, December 2016.

7. CROSS REFERENCES

Where applicable, sections of this TD P will provide a cross reference to the corresponding section of 32 CFR Part 2002 and will be indicated by "[§ 2002.xx]."

8. DEFINITION [§ 2002.4].

[2] NIST publications are accessible at https://beta.csrc.nist.gov/publications; CFRs are accessible at http://www.ecfr.gov/cgi-bin/text-idx?tpl=%2Findex.tpl; and EOs are accessible at https://www.federalregister.gov/executive-orders

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.

32 CFR Part 2002.4 contains additional relevant definitions.

9. POLICY and IMPLEMENTATION

Each bureau shall issue a CUI Policy and shall protect all CUI in accordance with national directives and this TD P, ensure that sharing partners exercise the same care, and remove any CUI-mandated controls on the information once it is decontrolled. These policies should include or identify all CUI routinely handled by bureau personnel and address the unique safeguarding or handing requirements for CUI Specified categories or subcategories. Removal of CUI controls does not constitute authorization to release the information. The absence of CUI designations is not dispositive for such purposes as FOIA processing. Decontrolling occurs when an authorized holder, consistent with this part 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. If there is significant doubt about whether information should be designated as CUI, it shall not be so designated (See section 15 for more additional information).

There will be a phased implementation of the CUI Program within Treasury. The date of full implementation of the program will be announced by the Treasury CUI Senior Agency Official (CUI SAO). Throughout implementation, legacy markings and safeguarding practices will exist at the same time but as implementation progresses, legacy markings and safeguarding practices will be phased out eventually.

10. RESPONSIBILITIES

The Assistant Secretary for Management (ASM) shall:

- Ensure Departmental senior leadership support
- Make adequate resources available to implement, manage, and comply with the requirements of the National CUI Program
- Designate and advise NARA of the Department's CUI SAO responsible for oversight of the Department's CUI Program implementation, compliance, and management, and include the SAO in all contact listings
- Advise NARA of any changes to the designated SAO
- Approve Departmental policies as needed to implement the CUI Program

The SAO for CUI shall:

Policies and Procedures:

- Develop and execute current Department-wide policies, plans, and procedures necessary to implement and manage a CUI program that complies with EO 13556 and 32 CFR Part 2002

- Develop and implement the Department's self-inspection program
- Establish a process to accept and manage challenges to CUI status (including improper or absence of marking) in accord with existing processes based in laws, regulations, and government-wide policies
- Establish processes and criteria for reporting and investigating misuse of CUI
- Establish processes for handling CUI decontrol requests submitted by authorized holders
- Establish a mechanism by which authorized holders (both inside and outside Treasury) can contact a designated representative for instructions when they receive unmarked or improperly marked information Treasury designated as CUI
- Submit to NARA any law, regulation, or government-wide policy not already incorporated into the CUI Registry that the agency proposes to use to designate unclassified information for safeguarding or dissemination controls
- Coordinate with NARA, as appropriate, any proposed law, regulation, or government-wide policy that would establish, eliminate, or modify a category or subcategory of CUI, or change information controls applicable to CUI

Training:

- Implement an education and training program pursuant to 32 CFR § 2002.30 to include monitoring for compliance with training requirements
- Ensure the training and education program for both basic and specified categories of CUI includes sufficient information that allows all Treasury personnel to understand and carry out their obligations with respect to protecting, storing, transmitting, transporting, and destroying CUI

Oversight/Management:

- Direct and oversee the Department's CUI Program
- Designate a CUI Program Manager (PM)
- Delegate, with concurrence from the ASM, operational responsibilities for the CUI Program to other Treasury program offices, as appropriate
- Assist in and respond to audits conducted by NARA

Reporting:

- Upon request of NARA, provide updates regarding the Department's CUI implementation efforts and overall program status
- Include a description of all waivers granted in the annual report to NARA, along with the rationale for each waiver and the alternative steps being taken to protect CUI within the Department (see section 31 below)

The CUI PM shall:

- Manage the day-to-day operations of Treasury's CUI Program as directed by the CUI SAO
- Coordinate CUI policy development and updates
- Serve as the Department's official representative to NARA on the Department's CUI Program operations and related matters, including submission of required reports
- Serve as the Department's official representative on the Interagency CUI Advisory Council to advise NARA on the development and issuance of policy and implementation guidance for the CUI Program
- Serve as the Department's most senior subject matter expert in CUI, advising Treasury bureaus on their CUI programs to ensure CUI operations comply with government-wide requirements
- Convey requirements for training and reporting to Treasury bureaus
- Consolidate status reports from the bureaus and forward Departmental reports to NARA
- Organize and oversee CUI training efforts
- Maintain an internal website accessible by all Treasury employees, contractor employees, detailees, and interns that contains information about the CUI Program, with a section for each bureau to list their frequently-encountered CUI categories and subcategories and special instructions

The Deputy Assistant Secretary for Information Systems and Chief Information Officer shall safeguard CUI in Treasury Systems by:

- Assessing Treasury systems that contain CUI
- Ensuring that all information technology systems that are used to process CUI meet the federal baseline of moderate confidentiality
- Incorporating appropriate security measures into enterprise IT systems that contain CUI
- Coordinating with the CUI SAO on IT system security to comply with CUI requirements
- Ensuring that information systems that process, store, or transmit CUI are in compliance with FIPS PUB 199 and 200, NIST SP 800-53, and other federal IT requirements
- Issuing guidance regarding acceptable methods of protecting CUI within IT systems and transmitting CUI from Treasury email systems
- Issuing guidance regarding acceptable methods of protecting CUI on public facing websites and in cloud based systems
- Ensuring information systems that contain CUI have the appropriate CUI Markings as per 32 CFR 2002

Bureau CUI PMs and Designated CUI Points of Contact (POC) and alternates shall:

- Complete all required CUI training
- Conduct oversight actions to ensure compliance within their area of responsibility and report findings at least annually to the Treasury CUI PM
- Serve as their office or organization's CUI subject matter expert, responding to most inquiries from their organizations and consulting with the CUI PM on questions beyond their expertise

- Ensure all personnel within their office or organization complete initial and recurring training as required and report the progress of training to the Treasury CUI PM
- Conduct annual self-inspections of their CUI Program, according to the guidance provided by the CUI PM, to reflect the progress of implementation and report the results of those self-inspections to the CUI PM (see Section 26 for additional information)
- Provide input from their respective offices on all other reporting requirements to the CUI PM to enable a Departmental response to NARA
- Report instances of potential CUI violation or infractions to the CUI PM and keep track of violations for reporting purposes
- Confirm their status as a CUI POC with the CUI PM on a semi-annual basis (by the dates designated by the CUI PM) and provide notification within five business days if their status changes

Contracting Officers and Contracting Officer Representatives (CORs) shall:

- Include the applicable federal and Departmental CUI security clauses in their assigned contracts
- Ensure contractors are aware of and understand the CUI security clauses in their contracts
- Include in all contracts, which may involve CUI, a clause requiring that the contractor comply with NIST SP 800-171 for any non-federal computer system they operate that contains CUI (see 32 CFR 2002.14(h)(2) for more information)
- Ensure contractors receive training on CUI within 60 days and before accessing CUI

Supervisors and Managers shall:

- Ensure that all personnel under their purview receive CUI training as required by this policy (i.e., initial, recurring, and *CUI Specified*)
- Ensure that all employees under his/her supervision appropriately manage, mark, and protect CUI in accordance with this TD P
- Verify that all physical safeguarding measures for individual workspaces are adequate for the protection of CUI (i.e., prevent unauthorized access) annually
- Comply with all CUI Guidance provided by Treasury and their respective bureaus
- Ensure that employees under his/her supervision report incidents to the bureau CUI PM for their area of responsibility

Employees, contractor employees, detailees, and interns shall:

- Complete all initial, recurring, and *CUI Specified* assigned CUI training within the required timeframes
- Manage, mark, and protect CUI in accordance with this TD P and national directives
- Ensure that sensitive information currently stored as legacy material that is annotated as For Official Use Only (FOUO), or Sensitive but Unclassified (SBU), or that contains other legacy security markings is re-marked as CUI before the information leaves the Department. Only markings that are contained in the NARA CUI Registry may be used to annotate CUI (See section 17 below)

- Ensure that any CUI that they destroy is in accordance with the guidelines contained in Section 14 (and may include the use of the Waste Destruction Facility located in the main Treasury building)
- Report incidents to the bureau CUI PM for their area of responsibility

The Treasury Senior Agency Official for Privacy (SAOP) shall:

- Coordinate with the CUI SAO and CUI PM on all Treasury policies and procedures relating to the Privacy Act and Personally Identifiable Information (PII) to ensure consistency with the CUI framework and requirements
- Ensure Treasury's compliance with privacy laws, regulations, and Treasury privacy policies applicable to CUI and this TD P

11. KEY ELEMENTS OF THE CUI PROGRAM

- The CUI Registry [§ 2002.10] is the online repository for all information, guidance, policy, and requirements on handling CUI, including everything issued by NARA. Among other information, the CUI Registry identifies all approved CUI categories and subcategories, provides general descriptions for each, identifies the basis for controls, establishes markings, and includes guidance on handling procedures.

- "*CUI Basic*" is the subset of CUI for which the authorizing law, regulation, or government-wide policy does not set out specific handling or dissemination controls. Agencies handle *CUI Basic* according to the uniform set of controls set forth in this TD P and the CUI Registry.

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

- CUI categories and subcategories [§ 2002.12]

    - CUI categories and subcategories are those types of information for which laws, regulations, or government-wide policies require or permit agencies to exercise safeguarding or dissemination controls, and which NARA has approved and listed in the CUI Registry
    - Treasury personnel may use only those categories or subcategories approved by NARA and published in the CUI Registry to designate information as CUI

12. SAFEGUARDING [§ 2002.14]

- The objective of safeguarding is to prevent the unauthorized disclosure of or access to CUI

- Unless different protection is specified in the CUI Registry, CUI (including CUI in burn bags) must be stored in a locked office, locked drawer, or locked file cabinet whenever it is left unattended. If cleaning or maintenance personnel are allowed into private offices after hours, CUI within those offices must be secured in a locked desk drawer or locked file cabinet.

- Individuals working with *CUI Specified* subcategories (e.g., Sensitive Security Information) must comply with the safeguarding standards outlined in the underlying law, regulation, or government-wide policy in addition to those described in this TD P

- Safeguarding During Working Hours. Persons working with CUI shall be careful not to expose CUI to others who do not have a lawful government purpose to see it. Cover sheets – Optional Form (OF) 901, OF 902, and OF 903 – may be placed on top of documents to conceal their contents from casual viewing. See Section 28 of this TD P. Treasury personnel may use cover sheets to protect CUI while they are in the vicinity of the information, but they must secure CUI in a locked location, such as a desk drawer, file cabinet, or office, whenever they leave the area.

- Other Precautions:

    - Treasury personnel should reasonably ensure that unauthorized individuals cannot access or observe CUI, or overhear conversations where CUI is discussed

    - CUI should be kept in a controlled environment which is defined as any area or space an authorized holder deems to have adequate physical or procedural controls (e.g., barriers and managed access controls) for protecting CUI from unauthorized access or disclosure

    - When outside a controlled environment, Treasury 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 protects the CUI from unauthorized access or observation

    - Treasury personnel should protect the confidentiality of CUI that is processed, stored, or transmitted on federal information systems in accordance with applicable Treasury policy or procedure

- Care While Traveling. CUI shall not be viewed while on public transportation where others may be exposed to it. In hotel rooms, CUI should be kept in a locked briefcase or room safe. CUI may be stored in a locked automobile only if it is in an envelope, briefcase, or otherwise covered from view. The trunk is the most secure location for storing CUI in an automobile.

- Bureaus may not require more restrictive safeguarding standards than those described in this TD P or 32 CFR Part 2002 for their contractors or other partners with whom they share CUI

13. CUI WITHIN INFORMATION SYSTEMS [§ 2002.14(g)]

- In accordance with FIPS PUB 199, *CUI Basic* is categorized at no less than the moderate confidentiality impact level. FIPS PUB 199 defines security impact levels for federal information and 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. Treasury may increase *CUI Basic*'s confidentiality impact level above moderate only within Treasury, including contractors operating an information system on behalf of Treasury, or by means of agreements between Treasury and other agencies. Treasury 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 Treasury.

- Information systems that process, store, or transmit CUI are of two different types:

    - A federal information system is an information system used or operated by a federal agency or by a contractor of an agency or other organization on behalf of an agency. Information systems that any entity operates on behalf of Treasury are subject to the requirements of the CUI Program as though they are Treasury systems, and Treasury may require these systems to meet the same requirements as Treasury's own internal systems.

    - A non-federal information system is any information system that does not meet the criteria for a federal information system. Treasury personnel may not treat non-federal information systems as though they are Treasury systems, so non-executive branch entities cannot be required to protect these systems in the same manner that the Treasury might protect its own information systems. Instead, entities employing non-federal information systems must follow the requirements of NIST SP 800-171 in order to protect *CUI Basic*, unless specific requirements are specified by law, regulation, or government-wide policy for protecting the information's confidentiality.

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

14. DESTRUCTION [§ 2002.14(f)]

- CUI may be destroyed:

    - 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. If the authority does not specify a destruction method, agencies must use one of the following methods:

    - 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*

    - Guidance for media sanitation and destruction applicable to Treasury information and information systems found in TD P 85-01, Appendix A (MP-6)

    - Any method of destruction approved for Classified National Security Information, as delineated in 32 CFR 2001.47, *Destruction*, or any implementing or successor guidance

15. SHARING OF CUI (Accessing and Disseminating) [§ 2002.16]

- General Policy (Access), Bureaus should disseminate and permit access to CUI, provided such access or dissemination:

    - Abides by the laws, regulations, or government-wide policies that established the CUI category or subcategory

    - Furthers a lawful government purpose

    - Is not restricted by an authorized limited dissemination control established by NARA

    - Is not otherwise prohibited by law

- 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. If there is significant doubt about whether it is appropriate to use a limited dissemination control, Treasury personnel should consult with and follow the designating agency's policy. If, after consulting the policy, significant doubt still remains, please consult with the CUI SAO for further guidance. Limited dissemination controls include: no foreign dissemination, federal employees only, federal employees and contractors only, no dissemination to contractors, dissemination list controlled, authorized for release to

certain nationals only, and display only. See Section 17 below for guidance on limited dissemination control markings.

- Agencies may not impose controls that unlawfully or improperly restrict access to CUI
- CUI may be shared with a non-executive branch or a foreign entity under the following conditions in addition to the requirements listed above:
    - 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
    - Whenever feasible, bureaus 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.
    - Foreign entity sharing [2002.16(a)(5)(iii)]. When entering into information-sharing agreements or arrangements with a foreign entity, Treasury personnel should encourage that entity to protect CUI in accordance with EO 13556; 32 CFR Part 2002; and the CUI Registry. Treasury 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.
    - 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-executive branch 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 Treasury is not the designating agency, Treasury personnel must report any non-compliance to the designating agency. [§ 2002.16(a)(6)]
- *CUI Basic* may be disseminated to persons and entities meeting the access requirements of this section. Bureaus may further restrict the dissemination of *CUI Basic* by using an authorized Limited Dissemination Control Marking published in the CUI Registry.
- Authorized recipients of *CUI Basic* may further disseminate the information to individuals or entities meeting and complying with the requirements of this CUI Program. *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). In addition, bureaus may further restrict dissemination of *CUI Specified* by using an authorized Limited Dissemination Control Marking published in the CUI Registry.

16. DECONTROL OF CUI [§ 2002.18]

- When control is no longer needed, Treasury should decontrol any CUI that it designates. This means the information should be removed from the protection of the CUI program as soon as practicable when the information no longer requires safeguarding or dissemination controls, unless doing so conflicts with the underlying authority.

- CUI may be decontrolled automatically for all or limited purposes upon the occurrence of one of the conditions below, or through an affirmative decision by the designator:

    - When laws, regulations or government-wide policies no longer require its control as CUI and the authorized holder has the appropriate authority under the authorizing law, regulation, or government-wide policy

    - When the designating agency decides to release the CUI to the public by making an affirmative, proactive disclosure

    - When an agency discloses it in accordance with an applicable information access statute, such as the Freedom of Information Act (FOIA) or the Privacy Act (when legally permissible), provided the designator's agency incorporates such disclosures into its public release processes

        - Disclosures under FOIA constitute CUI decontrol for all Treasury purposes

        - 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 (not for other Treasury purposes)

- A designating agency may also decontrol CUI:

    - In response to a request from an authorized holder to decontrol it

    - Concurrently with any declassification action under EO 13526 or any predecessor or successor order, as long as the information also appropriately qualifies for decontrol as CUI

- A bureau may designate in its CUI policies which personnel it authorizes to decontrol CUI, consistent with law, regulation, and government-wide policy

- Decontrolling CUI for purposes other than FOIA disclosure relieves the requirement to handle the information under the CUI Program, but does not constitute authorization for public release

- Treasury personnel must clearly indicate that CUI is no longer controlled when restating, paraphrasing, re-using, releasing to the public, or donating the CUI to a private institution. Otherwise, Treasury personnel do not have to mark, review, or take other actions to indicate the CUI is no longer controlled.

    - For relatively short documents, all CUI markings within a decontrolled CUI document shall be removed or struck though. For large documents, Treasury personnel may remove or strike through only those CUI markings on the first or cover page of the decontrolled CUI and markings on the first page of any attachments that contain CUI. They shall also mark or stamp a statement on the first page or cover page that the CUI markings are no longer applicable.

    - If Treasury personnel use decontrolled CUI in a newly created document, they must remove all CUI markings for the decontrolled information

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

- Authorized holders may request that the designating agency decontrol CUI that they believe should be decontrolled. See section 34 below, Challenges to Designation of Information as CUI.

- If an authorized holder publicly releases CUI in accordance with the designating agency's (non-Treasury designators) authorized procedures, the release constitutes decontrol of the information

- Unauthorized disclosure of CUI does not constitute decontrol

- Treasury personnel must not decontrol CUI in an attempt to conceal, or to otherwise circumvent accountability for, an unauthorized disclosure

- When laws, regulations, or government-wide policies require specific decontrol procedures, Treasury personnel 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. The Archivist decontrols records to facilitate public access pursuant to 44 U.S.C. 2108 and NARA's regulations at 36 CFR parts 1235, 1250, and 1256.

17. MARKING OF CUI [§ 2002.20]

- CUI markings listed in the CUI Registry are the only markings authorized to designate unclassified information requiring safeguarding or dissemination controls
- Treasury personnel and authorized holders must, in accordance with the implementation timelines established within the Department:
    - Discontinue all use of legacy or other markings not permitted or included in the CUI Registry
    - Uniformly and conspicuously apply CUI markings to all CUI exclusively in accordance with the CUI Registry, unless Treasury has issued a limited CUI marking waiver
- Information may not be marked as CUI:
    - 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
    - If the CUI is required by law, regulation, or government-wide policy to be made available to the public or if it has been released to the public under proper authority
- The lack of a CUI marking on information that qualifies as CUI does not exempt the authorized holder from abiding by applicable CUI marking (see Section 25 below) and handling requirements as described in the TD P and the CUI Registry
- When it is impractical for a bureau to individually mark CUI due to quantity or nature of the information, or when the Department 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 screen, or signs in storage areas or in containers.
- 32 CFR Part 2002, the CUI Registry, and NARA's supplemental guidance (CUI Marking Handbook) shall be followed for the marking of CUI on paper and electronic documents. The handbook was developed to assist authorized holders by providing examples of correctly marked CUI.

- The CUI banner marking. Designators of CUI must mark all CUI with a CUI banner marking. The content of the CUI banner marking must be inclusive of all CUI within the document and must be the same on each page. Banner markings must appear at the top of each page of any document that contains CUI, including email transmissions. Banner markings may include up to three elements:

    - The CUI control marking. The CUI control marking may consist of either the word "CONTROLLED" or the acronym "CUI," at the designator's discretion. The CUI control marking is mandatory for all CUI and, by itself, is sufficient to indicate the presence of *CUI basic* categories or subcategories. Authorized holders who designate CUI may not use alternative markings to identify or mark items as CUI.

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

    - Limited Dissemination Control Markings. NARA has published a list of several Limited Dissemination Control Markings that can be applied based on Treasury's own criteria. These markings will appear in the CUI Registry and will include such controls as FED ONLY (Federal Employees Only), NOCON (No dissemination to contractors), and DL ONLY (Dissemination authorized only to those individuals or entities on an accompanying distribution list). 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 that includes CUI

- Specific marking, disseminating, informing, distribution limitation, or warning statements that are required by underlying authorities also may be placed on the document, but not within the banner or portion markings. These markings or indicators must be placed on

the document as prescribed by the underlying law, regulation, or government-wide policy. Questions regarding the placement of such markings may be referred to the responsible authority for the information.

- CUI designation indicator (Mandatory). On the first page or cover page of all documents containing CUI, the person or office that designated the CUI (the designator) must be identified. This may be accomplished through a "Controlled by" line. Every effort should be made to identify a point of contact, office, or division within an organization.

- CUI decontrolling indicators. Where feasible, a specific decontrolling date or event shall be included with all CUI. This may be accomplished in a manner that makes the decontrolling schedule readily apparent to an authorized holder.

- Incorrectly marked documents. If Treasury personnel believe that CUI is marked incorrectly, they should provide notice of the error to their respective CUI POC within their organization and the disseminating entity or the designating agency.

18. PORTION MARKING (Optional) [§ 2002.20(f)]

- 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.

- Portion marking is not required, but it is permitted and encouraged 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

- If portion markings are used in any portion of a document, they must be used throughout the entire document. Refer to the CUI Marking Handbook for additional guidance.

19. COMMINGLING CUI MARKINGS WITH CLASSIFIED NATIONAL SECURITY INFORMATION (CNSI) MARKINGS [§ 2002.20(g)]

- When authorized holders include CUI in documents that also contain CNSI, the decontrolling provisions of the CUI Program apply only to portions marked as CUI. In addition, Treasury personnel must:

    - Portion mark all CUI to ensure that authorized holders can distinguish CUI portions from portions containing classified and uncontrolled unclassified information

    - Include the CUI control marking, *CUI Specified* category or subcategory markings, and any limited dissemination control markings in the overall banner marking

- The CUI Registry and the NARA CUI Marking Handbook contain specific guidance on marking CUI when commingled with CNSI

20. TRANSPORTING CUI [§ 2002.14(d) and 20(i)]

- CUI may be sent through the United States Postal Service or any commercial delivery service

- Bureaus should use in-transit automated tracking and accountability tools when sending CUI

- CUI may also be sent through interoffice or interagency mail systems

- Address packages and parcels that contain CUI for delivery only to a specific recipient, not to an office or organization. Do not put CUI markings on the outside of an envelope or package, or otherwise indicate on the outside that the item contains CUI.

- CUI should be double-wrapped so that the CUI will be sealed even if the outer package is breached.

21. TRANSMITTAL DOCUMENT MARKING REQUIREMENTS [§ 2002.20(j)]

- When a transmittal document accompanies CUI, the transmittal document must include, on its face, a distinctive notice that CUI is attached or enclosed. This serves to notify the recipient about the sensitivity of the document beneath the cover letter.

- The notice shall include the CUI marking ("CONTROLLED" or "CUI") along with the following or similar instructions, as appropriate:

    - "When enclosure is removed, this document is Uncontrolled Unclassified Information"

    - "When enclosure is removed, this document is (indicate control level);" or, "upon removal, this document does not contain CUI."

22. REPRODUCTION OF CUI [§ 2002.14(e)]

- CUI may be reproduced (e.g., copied, scanned, printed, electronically duplicated) in furtherance of a lawful government purpose (in a manner consistent with the CUI marking)

- When reproducing CUI documents on equipment such as printers, copiers, scanners, or fax machines, management officials 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.

23. WORKING PAPERS [§ 2002.20(k)]

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

- Working papers containing CUI must be marked the same way as the finished product containing CUI would be marked and as required for any CUI contained within them. Working papers must be protected as any other CUI. This applies whether or not the working papers will be shortly destroyed. When no longer needed, working papers shall be destroyed in accordance with section 14 above.

24. USING SUPPLEMENTAL ADMINISTRATIVE MARKINGS WITH CUI [§ 2002.20(l)]

- Supplemental administrative markings (*e.g.*, "Pre-decisional," "Deliberative," "Draft") may be used with CUI. The NARA CUI Marking Handbook provides examples of supplemental administrative markings.

- 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 [topic]. It is not yet an accepted policy." (This is an example only. The language may be changed to suit the topic.)

- Supplemental markings may not appear in the CUI banners, nor may they be incorporated into the CUI designating/decontrolling indicators or portion markings

- Supplemental administrative markings must not duplicate any CUI marking described in the CUI Registry

25. UNMARKED CUI [§ 2002.20(m)]

- Unmarked information that qualifies as CUI should be marked and treated appropriately as described in this TD P.

26. CUI SELF-INSPECTION PROGRAM [§ 2002.24]

- In accordance with 32 CFR § 2002.8(b)(4), Treasury will implement a Self-Inspection Program as follows:

    - The CUI PM, under the authority of the CUI SAO, shall provide technical guidance, training, and materials for Treasury bureaus to conduct reviews and assessments of their CUI Programs at least annually, and to report the results to the CUI PM as NARA requires

    - Following training of the designated CUI POCs, bureaus shall conduct annual self-inspections of their CUI Programs and report the results on a schedule determined by the CUI SAO. Bureaus shall include in the self-inspection any contractors that are under their purview by on-site inspections or by examining any self-inspections conducted by the contractors.

    - Following guidance and inspection materials received from the CUI PM, self-inspection methods, reviews, and assessments shall serve to evaluate program effectiveness, measure the level of compliance, and monitor the progress of CUI implementation

    - The CUI PM shall provide to the bureaus formats for documenting self-inspections and recording findings, and provide advice for resolving deficiencies and taking corrective actions

    - Results from the department-wide self-inspections shall inform updates to the CUI training provided to the bureaus

.

27. EDUCATION AND TRAINING [§ 2002.30]

- Every Treasury employee, official, detailee, intern, and contractor employee who may encounter CUI in their work shall complete initial CUI awareness training within 60 days of employment and prior to access to CUI. Refresher training shall be required every two years after the initial training. Treasury personnel must also take training for any *CUI Specified* categories or subcategories they have access to or for which they are required to safeguard.

- CUI training must ensure that personnel who have access to CUI receive training on designating CUI, relevant CUI categories and subcategories, the CUI Registry, associated markings, and applicable safeguarding, disseminating, and decontrolling policies and procedures. See NARA CUI Notice 2017-01 for specific training elements that must be conveyed in initial and refresher training.

28. CUI COVER SHEETS [§ 2002.32]

- Treasury personnel 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 for CUI. Optional Form (OF) 901, OF 902, and OF 903 are the only authorized CUI cover sheets. Cover Sheets may be obtained from the Office of Security Programs and may then be reproduced by user offices. OF 901 may also be ordered from GSA. OF 902 and OF 903 contain space to add subcategories or warning notices and may be downloaded from the NARA site as follows:

    - OF 901: https://www.archives.gov/cui/additional-tools
    - OF 902: https://www.archives.gov/cui/additional-tools
    - OF 903: https://www.archives.gov/cui/additional-tools

29. TRANSFERRING RECORDS TO NARA [§ 2002.34]

- When feasible, records containing CUI shall be decontrolled prior to transferring to NARA

- If records cannot be decontrolled before transferring to NARA, the following procedures shall be followed:

    - Indicate on a Transfer Request (TR) in NARA's Electronic Records Archives (ERA) or on an SF 258 paper transfer form, that the records should continue to be controlled as CUI (subject to NARA's regulations on transfer, public availability, and access; see 36 CFR parts 1235, 1250, and 1256)

    - For hard copy transfer, do not place a CUI marking on the outside of the container or envelope. Double-wrapping is not required, but if used, only the interior envelope should be marked as "Controlled" or "CUI."

- If status as CUI is not indicated on the TR or SF 258, NARA may assume the information was decontrolled prior to transfer, regardless of any CUI markings on the actual records. Therefore, Treasury personnel shall clearly indicate the CUI status (whether it is still active or decontrolled) prior to transfer.

30. LEGACY MATERIALS [§ 2002.36]

- Documents created prior to November 14, 2016 (and prior to Treasury CUI implementation) must be reviewed and re-marked if they contain information that qualifies as CUI. If an agency does not re-mark the legacy material, they must use an alternate permitted marking method.

- See Section 31 (below) for information on waivers regarding legacy documents

31. WAIVERS OF CUI REQUIREMENTS [§ 2002.38]

- Limited CUI marking waivers. When a bureau designates information as CUI but determines that marking it as CUI is excessively burdensome, the CUI SAO may approve waivers of all or some of the CUI marking requirements while the CUI remains within Treasury.

- Limited legacy material marking waivers. The CUI SAO may approve waivers of all or some of the CUI marking requirements while the CUI remains within Treasury, 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

- When an authorized holder re-uses any legacy information or information derived from legacy documents that qualifies as CUI, they must remove or 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

- In exigent circumstances,[3] the CUI SAO may waive certain requirements of the CUI Program for any CUI while it is within Treasury's possession or control, unless specifically prohibited by applicable laws, regulations, or government-wide policies.

- Exigent circumstances waivers may apply when Treasury 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.

- Waivers approved by the CUI SAO are valid only while the information remains within Treasury. CUI markings must be uniformly and conspicuously applied to all CUI prior to disseminating it outside Treasury unless otherwise specifically permitted by NARA.

- Per 32 CFR Part 2002.38(e), the CUI SAO 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 web sites

[3] Exigent circumstances exist when following proper procedures would cause an unacceptable delay due to the urgency of the situation.

32. CUI AND DISCLOSURE STATUTES [§ 2002.44]

- General policy. The fact that information is designated as CUI does not prohibit its disclosure if the disclosure is made according to criteria set out in a governing law

- CUI and the Freedom of Information Act (FOIA). FOIA may not be cited as a CUI safeguarding or disseminating control authority for CUI. When determining whether to disclose information in response to a FOIA request, the decision must be based upon the content of the information and applicability of any FOIA statutory exemptions, regardless of whether or not the information is designated or marked as CUI. There may be circumstances in which CUI may be disclosed to an individual or entity, including through a FOIA response, but such disclosure does not always constitute public release as defined by the CUI Program. Although disclosed via a FOIA response, the CUI may still need to be controlled while Treasury continues to hold the information, despite the disclosure, unless it is otherwise decontrolled (or the Department indicates in its policies that FOIA disclosure always results in public release and the CUI does not otherwise have another legal requirement for its continued control).

- CUI and the Whistleblower Protection Act. The CUI Program does not change or affect existing legal protections for whistleblowers. The fact that information is designated or marked as CUI does not determine whether an individual may lawfully disclose that information under a law or other authority, and does not preempt or otherwise affect whistleblower legal protections provided by law, regulation, EO or directive.

33. CUI AND THE PRIVACY ACT [§ 2002.46]

- The fact that records are subject to the Privacy Act of 1974 does not mean that the Privacy Act is the sole reason for marking the records as CUI. Information contained in Privacy Act systems of records may also be subject to controls under other CUI categories or subcategories and may need to be marked as CUI for that reason. In addition, when determining whether certain information must be protected under the Privacy Act or whether the Privacy Act allows an individual the right to access their information maintained in a system of records, the decision to release must be based upon the content of the information as well as Privacy Act criteria, regardless of whether the information is designated or marked as CUI. Decontrol of CUI for the limited purpose of making an individual's information available to them under the Privacy Act does not result in decontrol for any other purpose inconsistent with this TDP.

- Consult the CUI Registry to determine what PII must be marked as CUI

- In determining whether CUI markings are necessary and, if so, what markings are appropriate, Treasury bureaus and offices should consult all compliance documentation associated with a particular information system. These documents will assist in making appropriate CUI marking decisions for documents and records that include PII. These include:

- The System Security Plan and the FIPS 199 confidentiality, integrity, and availability risk level determinations for the system
- Any Paperwork Reduction Act compliance documentation completed prior to collection of information from the public
- The applicable NARA Records Management Schedule or General Records Schedule
- The applicable Privacy and Civil Liberties Impact Assessment which discusses:
  - The applicable Privacy Act SORN for the records maintained in the information system (which should also be consulted)
  - Any applicable information sharing agreements
  - Handling requirements mandated by law with respect to particular information in the system
  - With whom the information is shared internally and externally

34. CHALLENGES TO DESIGNATION OF INFORMATION AS CUI [§ 2002.50]

- Authorized holders of CUI who, in good faith, believe that a designation as CUI is improper or incorrect, or who believe they have received unmarked CUI, should notify the designating agency (POC identified on the document and/or the CUI PM) of this belief. Challenges may be made anonymously; and challengers cannot be subject to retribution for bringing such challenges.
- If the information at issue is involved in litigation, or the challenge to its designation or marking as CUI arises as part of litigation, whether the challenger may access the information will be addressed via the litigation process instead of by the CUI PM. Challengers should nonetheless notify the CUI PM of the issue through the Treasury process described below, and include its litigation connection.
- If any Treasury organization receives a challenge, the CUI POC for that organization shall work with the Treasury CUI PM to take the following measures:
  - Acknowledge receipt of the challenge
  - Provide an expected timetable for response to the challenger
  - Review the merits of the challenge with a subject matter expert
  - Offer an opportunity to the challenger to define a rationale for belief that the CUI in question is inappropriately designated

- Notify the challenger of the Department's decision
- Provide contact information of the official making the decision in this matter

- Until the challenge is resolved, the challenged CUI should continue to be safeguarded and disseminated at the control level indicated in the markings

- If a challenging party disagrees with the Department's response to a challenge, that party may use the dispute resolution procedures described in 32 CFR § 2002.52.

35. MISUSE OF CUI AND INCIDENT REPORTING [§ 2002.54]

- Bureau CUI PMs shall develop reporting mechanisms (e.g., 1-800 numbers, dedicated email addresses, helpdesk) and amend existing procedures for the timely reporting of incidents involving CUI in their areas of responsibility. Amended procedures must make clear the following:
    - Bureau helpdesks or other incident intake staff, contractor employees, and existing personally identifiable information (PII) and non-PII incident reviewers must receive CUI incident intake, handling and reporting training.
    - Existing scripts or guides Departmental Helpdesks use to perform intake and distribution of incidents and breaches involving PII and non-PII incidents should be updated to incorporate CUI issues (where applicable) when PII and non-PII incidents are reported.
    - Existing bureau and Departmental guidance should be revisited to ensure that the applicable bureau CUI PM is notified as necessary during the review and resolution of PII and non-PII incidents so the bureau CUI PM may ensure compliance with the TD and this TDP.
    - Some bureaus have different reporting mechanisms depending on whether an incident involves PII or non-PII. Other bureaus may have a single office that handles both PII and non-PII incidents.
    - The existing bureau team(s) that resolve PII and/or non-PII incidents shall obtain the details of the situation, coordinate with a subject matter expert regarding the severity of the incident, and report the results of the investigation to the applicable bureau CUI PM(s) within 48 hours of discovery.
    - Existing bureau team(s) that resolve PII and/or non-PII incidents should coordinate mitigation measures as appropriate within their management structure and provide regular status reports to the bureau CUI PM until mitigation efforts are complete.

- The bureau CUI PM, in conjunction with the CUI SAO, shall determine if sanctions are appropriate for violations of existing policy, or if other corrective action may be warranted (e.g., emphasis in training). Misuse of CUI that has been designated by another Executive Department or agency shall be reported to that agency by the offending organization's bureau's CUI PM.

36. SANCTIONS FOR MISUSE OF CUI [§ 2002.56]

- Misuse of CUI may 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.

- In addition, any sanctions established by laws, regulations, or government-wide policies governing certain categories or subcategories of CUI shall be applied.

37. PUBLICATION OF CUI

- Publication of CUI or its posting on public web sites or social media is prohibited unless the CUI has been properly decontrolled in accordance with section 16 above

- CUI content owners should routinely review Treasury websites and social media sites to ensure that CUI is not posted

38. REQUESTING NEW CATEGORIES OR SUBCATEGORIES OF CUI

- Treasury personnel who encounter information described in law, regulations, or government-wide policy that is not described in the CUI Registry may recommend that a new information category or subcategory be entered into the Registry

- Treasury personnel should submit their recommendation through their CUI POC. The CUI POC shall coordinate through their legal counsel's office and submit a recommendation to the CUI PM. The request should include:

    - A description of the information to be marked as CUI

    - The law(s), regulation(s), or government-wide policy(-ies) that apply

    - If a subcategory, the name of the category applying to the information

    - A suggested name, along with a suggested acronym for the category or subcategory

- The CUI PM, in coordination with the Office of General Counsel, will submit the recommendation to NARA