U.S. DEPARTMENT OF COMMERCE

OPBM-NP-18-001

Controlled Unclassified Information (CUI)

Guidelines

August 2019

CONTROLLED
UNCLASSIFIED
INFORMATION

TABLE OF CONTENTS

1. INTRODUCTION 4
2. PURPOSE 4
3. AUTHORITY 5
4. APPLICABILITY [32 CFR § 2002.22] 5
5. LIMITATIONS ON APPLICABILITY OF THIS GUIDE 5
6. REFERENCES 5
7. CROSS REFERENCES 6
8. DEFINITIONS [§ 2002.4]. 6
9. POLICY and IMPLEMENTATION 8
10. RESPONSIBILITIES 8
11. KEY ELEMENTS OF THE CUI PROGRAM 13
12. SAFEGUARDING AND STORAGE [§ 2002.14] 14
13. CUI WITHIN INFORMATION SYSTEMS [§ 2002.14(g)] 15
14. DESTRUCTION [§ 2002.14(f)] 16
15. SHARING OF CUI (Accessing and Disseminating) [§ 2002.16] 17
16. DECONTROL OF CUI [§ 2002.18] 18
17. MARKING OF CUI [§ 2002.20] 20
18. PORTION MARKING (Optional) [§ 2002.20(f)] 22
19. COMMINGLING CUI MARKINGS WITH CLASSIFIED NATIONAL SECURITY INFORMATION (CNSI) MARKINGS [§ 2002.20(g)] 23
20. TRANSPORTING CUI [§ 2002.14(d) and 20(i)] 23
21. TRANSMITTAL DOCUMENT MARKING REQUIREMENTS [§ 2002.20(j)] 23
22. REPRODUCTION OF CUI [§ 2002.14(e)] 24
23. WORKING PAPERS [§ 2002.20(k)] 24
24. USING SUPPLEMENTAL ADMINISTRATIVE MARKINGS WITH CUI [§ 2002.20(l)] 24
25. UNMARKED CUI [§ 2002.20(m)] 25
26. CUI SELF-INSPECTION PROGRAM [§ 2002.24 and § 2002.8] 25

27. EDUCATION AND TRAINING [§ 2002.30] 25
28. CUI COVER SHEETS [§ 2002.32] 26
29. TRANSFERRING RECORDS TO NARA [§ 2002.34] 26
30. LEGACY MATERIALS [§ 2002.36] 26
31. WAIVERS OF CUI REQUIREMENTS [§ 2002.38c] 28
32. CUI AND DISCLOSURE STATUTES [§ 2002.44] 29
33. CUI AND THE PRIVACY ACT [§ 2002.46] 29
35. CHALLENGES TO DESIGNATION OF INFORMATION AS CUI [§ 2002.50] 30
36. MISUSE OF CUI AND INCIDENT REPORTING [§ 2002.54] 31
37. SANCTIONS FOR MISUSE OF CUI [§ 2002.56] 32
38. PUBLICATION OF CUI 33
39. REQUESTING NEW CATEGORIES OF CUI 33

U.S. Department of Commerce (DOC) Policy OPBM-NP-18-0001

Controlled Unclassified Information (CUI) Guidelines

These guidelines provide further directions to all bureaus, offices, and organizations in the DOC for compliance with DOC OPBM-NP-18-0001 and are incorporated therein.

1. INTRODUCTION

In November 2010, the President issued Executive Order (E.O.) 13556, *Controlled Unclassified Information* (CUI), to "establish an open and uniform program for managing [unclassified] information that requires safeguarding or dissemination controls" pursuant to and consistent with law, regulations, and Government-wide policies.

Prior to that time, more than 100 different markings for such information existed across the executive branch. This *ad hoc*, agency-specific approach to policies, procedures, and markings to safeguard and control this information, such as information that involves privacy, security, proprietary business interests, and law enforcement investigations, created inefficiency and confusion, failed to adequately safeguard information requiring protection, and created impediments to authorized information-sharing. The fact that these agency-specific policies are often hidden from public view has only aggravated these issues.

As a result, E.O. 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 on its website that serves as the authoritative reference for all CUI categories and markings.

2. PURPOSE

These guidelines and the DOC CUI Policy implement E.O. 13556 and 32 CFR Part 2002, which institute national policy on the handling, safeguarding, and control of CUI. CUI is any information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that is required or specifically permitted to be protected under law, regulation, or Government-wide policy. Classified information is not part of the CUI Program as E.O. 13526 is the directive for Classified National Security Information.

All unclassified information throughout the executive branch that requires any safeguarding or dissemination control is CUI**.** In other words, CUI shall serve as the exclusive designation

for identifying unclassified information throughout the executive branch. No safeguarding or dissemination controls for unclassified information may be implemented unless they are consistent with the CUI Program.

3. AUTHORITY

This Guide is issued under the authority of DOC Policy OPBM-NP-18-0001, *Controlled Unclassified Information (CUI) Policy*, dated August 2019.

4. APPLICABILITY [32 CFR § 2002.22]

This guide sets forth standards for the handling, marking, safeguarding, destruction, and decontrolling of CUI for the DOC enterprise. This policy applies to all personnel, including employees, contractor employees, detailees, guest researchers, interns, and other associates, who may encounter CUI in the performance of official DOC duties.

The provisions of this policy shall not be construed to interfere with or impede the authorities or independence of the DOC Inspector General as provided for in the Inspector General Act of 1978, as amended, or other statutory OIG reporting obligations.

5. LIMITATIONS ON APPLICABILITY OF THIS GUIDE

As limited by 32 CFR § 2002.22, DOC CUI bureau policies do not apply to entities outside the agency unless a law, regulation, or Government-wide policy requires or permits the controls contained in the agency policy to do so and the CUI Registry lists that law, regulation, or Government-wide policy as a CUI authority. DOC CUI bureau policies may apply to non-executive branch CUI recipients through incorporation into agreements (§2002.1(f) and §2002.22).When entering into agreements, DOC organizations shall not include additional requirements or restrictions on handling CUI other than those permitted in the Executive Order, 32 CFR Part 2002, or the CUI Registry.

6. REFERENCES[1]

E.O. 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

[1] 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 E.O.s are accessible at https://www.federalregister.gov/executive-orders

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 policy will provide a cross reference to the corresponding section of 32 CFR Part 2002 and will be indicated by "[§ 2002.xx]."

8. DEFINITIONS [§ 2002.4].

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 party 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-executive branch 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 32 CFR Part 2002, and approved DOC CUI policy and guidelines.

Controls are safeguarding or dissemination controls that a law, regulation, or Government-wide policy requires or permits agencies to use when handling CUI. The authority may specify controls it requires or permits the agency to apply, or the authority may generally require or permit agencies to control the information (in which case the agency applies controls from the E.O., 32 CFR Part 2002, and the CUI Registry).

Controlled is an alternative banner marking used by some departments and agencies to indicate that the presence of CUI information is contained in the document. "Controlled" is equivalent to the banner marking "CUI". However, DOC will not use "Controlled" as an alternative banner marking.

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

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 with safeguarding or dissemination controls.

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

CUI Specified is the subset of CUI in which the authorizing law, regulation, or Government-wide policy contains specific handling controls that requires or permits agencies to use procedures and protections that exceed 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 guidance.

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

Decontrolling occurs when an authorized holder, consistent with the CUI regulations 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 Part 2002 and the CUI Registry, determines that a specific item of information falls into a CUI category.

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

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

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

Legacy material is unclassified information that an agency marked as restricted from access or dissemination in some way, or otherwise controlled, prior to the CUI Program.

Limited Dissemination Controls is 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 these guidelines, the CUI regulations, E.O. 13556, 32 CFR Part 2002, the CUI Registry, agency CUI policy, or the applicable laws, regulations, and Government-wide policies that govern the affected information. This may include intentional violations or unintentional errors in safeguarding or disseminating CUI. This may also include designating or marking information as CUI when it does not qualify as CUI.

Uncontrolled Unclassified Information or UUI is information that neither the E.O. 13556 nor the authorities governing classified information 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.

32 CFR § 2002.4 contains additional relevant definitions.

9. POLICY and IMPLEMENTATION

Each bureau may issue specific bureau requirements and shall protect all CUI in accordance with DOC policy and guidelines to ensure that sharing partners exercise the same care and remove any CUI controls on the information once it is decontrolled. These specific bureau requirements shall include or identify all CUI that is routinely handled by bureau personnel. The DOC CUI webpage shall be the central repository for the CUI Policy, these guidelines, and any specific bureau requirements.

There will be a phased, high-level implementation plan developed by the DOC CUI Program Office and posted to the DOC CUI website. This plan will include the targeted date of full implementation of the program as directed by the DOC 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

Agency Heads shall: [§ 2002.8]

- Ensure senior leadership support of CUI Program policy
- Make adequate resources available to implement, manage, and comply with the requirements of the National CUI Program
- Designate and advise NARA of the DOC's CUI SAO responsible for oversight of the DOC's CUI Program implementation, compliance, and management, and include the SAO in all contact listings

- In collaboration with the DOC Office of Security, conduct physical self-inspections of areas storing and processing CUI materials
- Advise NARA of any changes to the designated SAO
- Approve policies as needed to implement the CUI Program

The DOC Chief Information Officer (CIO) is the designated SAO for CUI and shall: [§2002.8]

- Direct and oversee the DOC's CUI Program
- Designate a CUI Program Manager (PM)
- Ensure the DOC has CUI implementing policies and plans, as needed
- Develop and execute current DOC-wide policies and procedures necessary to manage a CUI program that complies with E.O. 13556 and 32 CFR Part 2002
- 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 include sufficient information that allows all personnel to understand and carry out their obligations with respect to protecting, storing, transmitting, transporting, and destroying CUI
- Upon request of NARA, provide updates of the DOC's CUI implementation efforts
- Assist in and respond to audits conducted by NARA
- Include a description of all waivers granted in the annual report to NARA, along with the rationale for each waiver, where applicable, and the alternative steps being taken to protect CUI within the DOC (see section 31 below)
- Develop and implement the DOC'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
- Notify authorized recipients and the public of any waivers the DOC grants (unless notice is otherwise prohibited by law, regulation, and government-wide policy), and separately notify NARA
- 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 and the DOC CUI PM 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.
- Establish processes for handling CUI decontrol requests submitted by authorized holders

- Establish a mechanism by which authorized holders (both inside and outside DOC) can contact a designated representative for instructions when they receive unmarked or improperly marked information DOC designated as CUI

The CUI PM shall:

- Manage the day-to-day operations of DOC's CUI Program as directed by the CUI SAO
- Coordinate CUI policy development and updates
- Serve as the DOC's official representative to NARA on the DOC's CUI Program operations and related matters, including submission of required reports
- Serve as the DOC'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 DOC's most senior subject matter expert in CUI, advising DOC bureaus on their CUI programs to ensure CUI operations comply with government-wide requirements
- Investigate and lead mitigation efforts or assign personnel to investigate and lead mitigation efforts in coordination with the DOC bureaus for incidents involving CUI. Inform the CUI SAO of any significant CUI incidents as well as any incident trends found within the DOC or nationally
- Issuing guidance regarding acceptable methods for: protecting CUI within IT systems, transmitting CUI from DOC information systems, physical protections, and the destruction of CUI materials
- Convey requirements for training and reporting to DOC bureaus
- Consolidate status reports from the bureaus and forward DOC reports to NARA
- Organize and oversee CUI training efforts
- Maintain an internal website available for all employees to use that contains information about the CUI Program, with a section for each bureau to list their frequently-encountered CUI categories and special instructions
- In collaboration with the DOC Office of Security, update and maintain the DOC Security Manual, Chapter 35 to include CUI protocols, including:
  - Marking
  - Handling
  - Dissemination, access, and transmission
  - Storage requirements
  - Decontrolling and destruction
  - Incident reporting

The Bureau Chief Information Officers shall safeguard CUI in DOC Systems by:

- Assessing DOC systems that contain CUI

- Ensuring that all federal information technology systems that are used to process CUI are categorized at no less than the federal baseline of moderate confidentiality impact level per FIPS PUB 199
- Coordinating with the CUI SAO and Department Chief Information Security Officer (CISO) on IT system security to comply with CUI requirements
- Ensuring the agency applies appropriate security requirements and controls from FIPS PUB 199 and 200 and NIST SP 800-53 for Federal information systems that process, store, or transmit CUI
- Ensuring the agency applies NIST SP 800-171 when establishing security requirements to protect CUI's confidentiality on non-federal information systems unless the information involved prescribes specific safeguarding requirements or unless the agreement establishes requirements to protect CUI at higher than moderate confidentiality
- Issuing guidance regarding acceptable methods of protecting CUI within IT systems and transmitting CUI from DOC 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

Heads of Bureaus or their Designees shall:

- Ensure that the bureau has the ability to destroy CUI when DOC no longer needs the information, and DOC records disposition schedules no longer require retention of the records
- Destroy CUI, including CUI in electronic form, in a manner that makes it unreadable, indecipherable, and irrecoverable in accordance with NIST SP 800-88, Guidelines for Media Sanitization
- Ensure that physical materials that contain CUI have appropriate CUI markings as per 32 CFR § 2002.20

Bureau 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 DOC 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 bureaus complete initial and annual training as required and report the progress of training to the DOC 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 DOC-wide response to NARA
- Report instances of potential CUI misuse, violation or infractions in accordance with the DOC Computer Incident Response Plan and keep track of violations for reporting purposes, the CUI PM will be notified through the incident response process
- 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, Contracting Officer Representatives (CORs), and Agreement Managers shall:

- Include the applicable security clauses and standards in their assigned contracts
- Identify the types of CUI the agreement contains
- Include the appropriate CUI requirements of this policy in all agreements
- Ensure contractors receive training on CUI within 30 days of contract award or prior to accessing CUI, whichever occurs first.

Supervisors and Managers shall:

- Review and ensure that all CUI products are properly marked in accordance with this policy, as needed
- Verify that all physical safeguarding measures for individual workspaces are adequate for the protection of CUI (i.e., prevent unauthorized access) annually
- Verify that all electronic safeguarding measures are adequate for the protection of CUI (i.e., prevent unauthorized access) annually
- Ensure that all personnel under their purview receive CUI training as required by this policy
- Comply with CUI Guidance provided by DOC and their respective bureaus

DOC personnel, including employees, contractor employees, detailees, guest researchers, interns and other associates shall:

- Complete all initial, recurring, and *CUI Specified* assigned CUI training within the required timeframes
- Manage, mark, and protect CUI in accordance with this policy and national directives
- Ensure that sensitive information currently stored as legacy material that is annotated as For Official Use Only (FOUO), Sensitive But Unclassified (SBU), or that contains other legacy security markings is re-marked as CUI before the

information leaves the DOC. Only markings that are contained in the NARA CUI Registry may be used to annotate CUI (see Section 17 below)
- Report incidents as needed

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

- Advise the CUI SAO and CUI PM on all policies, procedures, laws, regulations, and guidance relating to the Privacy Act and Personally Identifiable Information (PII) and coordinate with the CUI SAO and CUI PM to ensure consistency with the CUI framework and requirements
- Ensure DOC's compliance with privacy laws, regulations, and privacy policies applicable to CUI and this policy
- The DOC SAOP may delegate this function to the Bureau Privacy Officer.

The DOC Chief Freedom of Information Act (FOIA) Officer shall:
- Advise the CUI SAO and CUI PM on all policies, procedures, laws, regulations, and guidance pertaining to the disclosure of information under the FOIA and coordinate with the CUI SAO and CUI PM to resolve any conflicts with the CUI framework and CUI requirements
- The DOC Chief FOIA Officer may delegate this function to Bureau FOIA Officers.

The Chief Data Officer (CDO) or equivalent shall consult, as necessary, with the SAO for CUI and the CUI PM to ensure appropriate safeguards are applied to protect CUI in Departmental digital assets.

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, 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 32 CFR Part 2002 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 exceed 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 [§ 2002.12]

- CUI categories 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
- Personnel may use only those categories approved by NARA and published in the CUI Registry to designate information as CUI

12. SAFEGUARDING AND STORAGE [§ 2002.14]

The objective of safeguarding is to prevent the unauthorized disclosure of or access to CUI. These guidelines set forth the minimum standards for safeguarding; however, bureaus may adopt specific bureau requirements.

Unless different protection is specified in the CUI Registry, documents and removable storage containing CUI must be password protected or otherwise stored in a locked office, locked drawer, or locked file cabinet whenever it is 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* must comply with the safeguarding standards outlined in the underlying law, regulation, or government-wide policy in addition to those described in this policy.

Safeguarding During Working Hours. Persons working with CUI shall be careful not to expose CUI to unauthorized users or others who do not have a lawful government purpose to see it. Cover sheets may be placed on top of documents to conceal their contents from casual viewing. See Section 28 of this policy. Personnel may use cover sheets to protect CUI document while in use, but must secure CUI documents in a locked location, such as a desk drawer, file cabinet, or office, when not in use or under observation, or filed for retention.

Other Precautions:

- 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.

- If authorized to remove CUI from a controlled environment, personnel must keep CUI under their direct control at all times or protect it with at least one physical barrier and reasonably ensure that they or the physical barrier protects the CUI from unauthorized access or observation.

Care While Traveling. All reasonable measures shall be taken (e.g. secure transmission, approved electronic USB or other method authorized by section 20 below) to mitigate risk and limit the necessity to hand carry CUI while in official travel status. CUI shall not be viewed while on public transportation where others may be exposed to it. In hotel rooms, CUI shall be stored in a locked briefcase or room safe when not in use. 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.

Care During Foreign Travel.

Specific instructions for handling and safeguarding of sensitive information, including CUI, is contained in Chapter 35 of the Department of Commerce Manual of Security Policies and Procedures.

Unless allowed by law, regulation or government-wide policy, bureaus may not require more restrictive safeguarding standards than those described in this policy or 32 CFR Part 2002 for their contractors or other partners with whom they share CUI.

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

IT systems containing CUI must minimally meet the federal baseline of moderate.

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. DOC may increase *CUI Basic*'s confidentiality impact level above moderate only within DOC, including contractors operating an information system on behalf of DOC, or by means of agreements between DOC and other agencies or non-executive branch entities. DOC 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 DOC.

Information systems that process, store, or transmit CUI are of two different types: [§2002.4(h)]

- 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 DOC are subject to the requirements of the CUI Program as though they are DOC systems, and DOC may require these systems to meet the same requirements as our own internal systems.

- A non-federal information system is any information system that does not meet the criteria for a federal information system. Personnel may not treat non-federal information systems as though they are DOC systems, so non-executive branch entities cannot be required to protect these systems in the same manner that the DOC might protect its own information systems. Instead, personnel must inform entities employing non-federal information systems that they must follow the requirements of NIST SP 800-171 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 applicable to DOC contractors and other non-executive branch entities that receive CUI incidental to providing a service or product to the government must meet if they have DOC CUI on their computer systems.

National Security Systems authorized to store, process, and/or transmit classified information are considered compliant with the necessary protections of CUI.

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* 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,* or NARA, *CUI Notice 2017-02: Controlled Unclassified Information (CUI) and Multi-Step Destruction Process.*
- Any method of destruction approved for Classified National Security Information, as delineated in 32 CFR 2001.47, *Destruction,* or any implementing or successor guidance.
- National Security Agency approved devices for device sanitization are required.

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

Agencies 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 Executive Agency; and,
- 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, personnel should consult with and follow the designating agency's policy. If, after consulting the policy, significant doubt still remains, please consult the CUI SAO for additional guidance. Limited dissemination control markings (LDCM) may be used for: 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. Bureaus are encouraged to use the dissemination list-controlled designation to limit access to particular individuals, offices, or organizations as deemed appropriated.

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 intended recipients are authorized to receive the CUI and understand safeguarding and handling requirements.
- 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 E.O. 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, such as Foreign Guest Researchers, personnel should encourage that entity to protect CUI in accordance with E.O. 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 objective 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; non-executive branch entities should familiarize themselves with the distinction between CUI Basic and CUI Specified information, and the markings and handling procedures for each, because non-executive branch entities and other authorized holders of CUI will be responsible for handling CUI in compliance with the requirements of this rule and the CUI Registry, through a forthcoming FAR clause. The rule's applications to non-executive branch entities imposes new potential liability. The misuse of CUI by non-executive branch entities 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 DOC is not the designating agency, 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. DOC may further restrict the dissemination of *CUI Basic* by using an authorized LDCM published on 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). As in the case of *CUI Basic*, *CUI Specified* may further restrict the dissemination of *CUI Specified* through the use of authorized LDCMs.

16. DECONTROL OF CUI [§ 2002.18]

When control is no longer needed, and as permitted by law, regulation, or government-wide policy, DOC 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 law, regulation, or government-wide policy.

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

    - Disclosure under FOIA does not automatically constitute CUI decontrol for all purposes. For more information, see Section 32 of these Guidelines.

    - 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 purposes)

When indicated by a decontrol marking specifying a decontrol date or event, CUI is decontrolled without further review by the originator.

- 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 E.O. 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.

- 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, 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 through. For large documents, 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 personnel use decontrolled CUI in a newly created document, they must remove all CUI markings for the decontrolled information. When indicated by a decontrol marking specifying a decontrol date or event, CUI is decontrolled without further review by the originator.

Once decontrolled, any public release of information that was formerly CUI must be in accordance with applicable law and 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 35 below, Challenges to Designation of Information as CUI.

If an authorized holder publicly releases CUI in accordance with the designating agency's (not DOC) authorized procedures, the release constitutes decontrol of the information.

Unauthorized disclosure of CUI does not constitute decontrol.

Personnel must not decontrol CUI to conceal, or to otherwise circumvent accountability for, an unauthorized disclosure.

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

Records Management Note: The Archivist of the United States may decontrol records transferred to the National Archives and Records Administration (NARA) in accordance with 32 CFR § 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. When feasible, CUI is decontrolled prior to the transfer of records to the NARA. When decontrol is not feasible prior to transfer, the CUI status of the information is indicated on a Transfer Request or an SF 258 paper form. Any other indication of CUI status, such as markings on the container, are not valid.

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.

Personnel and authorized holders must, in accordance with the implementation timelines established within the DOC:

- 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 DOC has issued a limited CUI marking waiver

Information may not be designated 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; or,
- 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 policy 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 DOC has issued a limited CUI marking waiver, authorized holders must make recipients aware of the information's CUI designation 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 NARA 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, if authorized. Banner markings may include up to three elements:

- The CUI control marking. The CUI control marking shall consist of the acronym "CUI". The CUI control marking is mandatory for all CUI and, by itself, is sufficient to indicate the presence of *CUI basic* categories. Authorized holders who designate CUI may not use alternative markings to identify or mark items as CUI.
- CUI category markings (mandatory for *CUI Specified*). If any part of a document contains *CUI Specified*, then the applicable category marking must appear in the banner, preceded by a "SP- " to indicate the specified nature of the category (e.g., CUI//SP-PCII). The CUI control marking, and any category markings are separated by a double forward slash (//). When including multiple categories in the banner they

must be alphabetized, with specified categories appearing before any basic categories. Multiple categories in a banner line must be separated by a single forward slash (/).

- Limited Dissemination Control Markings. NARA has published a list of Limited Dissemination Control Markings that can be applied based on DOC'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.

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 clear to an authorized holder.

Incorrectly marked documents. If 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 specific 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 strongly 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. All portions or sections must be portion marked, even those that do not contain CUI. Sections that do not contain CUI should be marked with as Uncontrolled Unclassified Information, designated with a [U].

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, 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.

Whether originally generated, derived, or reproduced by someone with an active clearance and a need to know, pursuant to E.O. 13526, documents which contain both CUI and NSI shall be classified at the highest level of the information contained therein. All precautions necessary to properly mark, disseminate, transport, transmit, reproduce, and store those documents as specified in Section III of the Manual for Security.

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)]

In-transit tracking may be required by a bureau for CUI. CUI may be sent through the United States Postal Service or any commercial delivery service that offers in-transit automated tracking and accountability tools. As an example, all Title 13 survey and statistical information requires in-transit tracking.

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.

Double wrapping CUI when it is being transported may be required by a bureau. As an example, all Title 13 survey and statistical information requires double wrapping.

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 ("CUI") along with the following or similar instructions, as appropriate:

- "When enclosure is removed, this document is Uncontrolled Unclassified Information (UUI)"
- "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 shall be marked and treated appropriately as described in this policy.

26. CUI SELF-INSPECTION PROGRAM [§ 2002.24 and § 2002.8]

In accordance with 32 CFR § 2002.8(b)(4), DOC 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 DOC 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 DOC-wide self-inspections shall inform updates to the CUI training provided to the bureaus.

27. EDUCATION AND TRAINING [§ 2002.30]

Every DOC employee, official, detailee, guest researcher, intern, and contractor employee who may encounter CUI in their work shall complete initial CUI awareness training within 30 days of employment and prior to access. Refresher training shall be required annually after the initial training. Personnel must also take training for any *CUI Specified* categories 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, the CUI Registry, associated markings, and applicable safeguarding, disseminating, and decontrolling policies and procedures. See NARA CUI Notice 2018-02 for specific training elements that must be conveyed in initial and refresher training.

28. CUI COVER SHEETS [§ 2002.32]

Personnel may use cover sheets to identify CUI and to serve as a shield to protect the attached CUI from inadvertent disclosure.

Cover sheet use may be required by a bureau for CUI. If a cover sheet is used, Standard Form (SF) 901 is the only authorized CUI cover sheet. Cover Sheets may be obtained from GSA or downloaded from the NARA CUI site and may then be reproduced by user offices.

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, personnel shall clearly indicate the CUI status (whether it is still active or decontrolled) prior to transfer.

30. LEGACY MATERIALS [§ 2002.36]

As a natural consequence of phased implementation, legacy markings, or any markings that were previously used to identify information that should be designated as CUI, and CUI markings will exist at the same time.

Documents created prior to November 14, 2016 (and prior to DOC CUI implementation) must be reviewed and re-marked if they contain information that qualifies as CUI and if the information is reused and expected to be transmitted outside the DOC. If the legacy material is not remarked, an alternate permitted marking method must be used.

The following protocols shall guide bureaus in the proper handling of legacy information when it is encountered during implementation of the CUI Program:

For information recipients:

1.Receiving marked legacy information when the recipient HAS implemented the CUI Program.

- If the receiving agency plans to reuse or transmit the legacy marked information to another agency, then it must evaluate the information and remark it as CUI as appropriate.
    - If applicable, the receiving agency must also adhere to any agency marking waivers as they apply to internal dissemination.
    - If applicable, the receiving agency should apply any appropriate Limited Dissemination Control Markings (LDCMs).
- Receiving agencies should NOT reuse legacy markings, such as FOUO or SBU, on new documents that are derived from marked legacy information.
- Agencies should contact the originator of the material if they have any questions.

2. Receiving information marked as CUI when the recipient HAS NOT implemented the CUI Program.
    - Transmitting agencies may feel some trepidation about the security of their information when sending it to another agency that has not implemented the CUI Program, as the recipient may not inherently protect this information to the same standards outlined in the CUI Program.
        - For this reason, the transmitting agency may wish to directly convey safeguarding requirements for this information to the receiver. Agencies without a CUI policy must handle incoming CUI in accordance with how the receiving agency protects sensitive documents.
    - Recipients must then protect this information in accordance with any safeguarding guidelines from the originators of the material, individual agency policy, and/or any Limited Dissemination Controls.
    - Receiving agencies should NOT remove CUI markings from the information.
    - Agencies should contact the originator of the material if they have any questions.

For information transmitters:

3. Transmitting marked legacy information when the recipient HAS implemented the CUI Program.
    - Transmitting agencies must provide a point of contact with the information in case the recipient has questions about safeguarding the material.
    - Any special handling requirements associated with the information, such as limited dissemination controls, should be conveyed through transmittal or in a manner apparent to the recipient of the information.

4. Transmitting information marked as CUI when the recipient HAS NOT implemented the CUI Program
   - The transmitting agency must keep its CUI markings on the information.
   - NARA recommends that if CUI Specified or Limited Dissemination Controls are contained in the transmission of the information, the sender should also include a description of the safeguarding or dissemination requirements related to the information.

31. WAIVERS OF CUI REQUIREMENTS [§ 2002.38c]

The CUI SAO may approve waivers of all or some of the CUI marking requirements while the CUI remains within DOC, 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,[2] the CUI SAO may waive certain requirements of the CUI Program for any CUI while it is within DOC's possession or control, unless specifically prohibited by applicable laws, regulations, or government-wide policies.

Exigent circumstances waivers may apply when DOC 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 DOC. CUI markings must be uniformly and conspicuously applied to all CUI prior to disseminating it outside DOC 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

[2] Exigent circumstances exist when the CUI SAO determines that following proper procedures would cause an unacceptable delay due to the urgency of the situation.

32. CUI AND DISCLOSURE STATUTES [§ 2002.44]

The fact that information is designated as CUI does not prohibit its disclosure to a DOC employee, official, detailee, guest researcher, intern, or contractor employee if the disclosure is made according to criteria set out in a governing law or regulation.

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 or Privacy Act request and 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 DOC continues to hold the information, despite the disclosure, unless it is otherwise decontrolled (or the Bureau FOIA Officer indicates that FOIA disclosure 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, E.O. 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 records should be marked as CUI. Information contained in Privacy Act systems of records may also be subject to controls under other CUI categories 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 DOC policy.

34. CUI AND PERSONALLY IDENTIFIABLE INFORMATION (PII)

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, DOC 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 (SSP) and the FIPS 199 confidentiality, integrity, and availability risk level determinations for the system,
- Any Paperwork Reduction Act (PRA) compliance documentation completed prior to collection of information from the public,
- The applicable NARA Records Management Schedule or General Records Schedule (GRS), and
- The applicable Privacy Impact Assessment (PIA) which discusses:
    - The applicable Privacy Act System of Records Notice (SORN) for the records maintained in the information system (which should also be consulted) with whom the information may be shared with internally and externally and any applicable information sharing agreements.
    - Handling requirements mandated by law with respect to particular information in the system.
    - The PII Confidentiality Impact Rating for the system and notice and consent opportunities for individuals providing information in the system.

35. 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 process described below and include its litigation connection.

If any DOC organization receives a challenge, the CUI POC for that organization shall work with the DOC 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 DOC's decision, and
- Provide contact information of the official making the decision in this matter.

Until the challenge is resolved, the challenged CUI, including challenges to unmarked CUI, should continue to be safeguarded and disseminated at the appropriate control level indicated in the markings or presumed category.

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

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

Bureaus shall develop reporting mechanisms (e.g., 1-800 numbers, dedicated email addresses) and procedures for the timely reporting of incidents involving CUI in their areas of responsibilities.

Suspected or confirmed misuse of CUI shall be reported via the bureau's incident response process and to the bureau's CUI POC immediately. The CUI POC 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 CUI PM within 48 hours of discovery. The CUI POC should coordinate mitigation measures as appropriate within their incident response and management structures and provide regular status reports to the CUI PM until mitigation efforts are complete.

Reportable CUI incidents include, but are not limited to:

- Any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of CUI.
- Any knowing, willful or negligent action to designate information as CUI contrary to the requirements of Executive Order 13556, and its implementing directives.
- Any incident involving computer or telecommunications equipment or media that may result in disclosure of CUI to unauthorized individuals, or that results in unauthorized modification or destruction of CUI system data, loss of CUI computer system processing capability, or loss or theft of CUI computer system media.
- Any incident involving the processing of CUI on computer equipment that has not been specifically approved and accredited for that purpose by an authorized official.
- Any incident involving the shipment of CUI by an unapproved method, or any evidence of tampering with a shipment, delivery, or mailing of packages containing CUI.
- Any incident in which CUI is not stored by an approved means.
- Any incident in which CUI is inadvertently revealed to or released to a person not authorized access.
- Any incident in which CUI is destroyed by unauthorized means.
- Any incident in which CUI is reproduced without authorization or contrary to specific restrictions imposed by the originator.
- Any incident in which CUI is shared contrary to an applied dissemination control marking.
- Any other incident in which CUI is not safeguarded or handled in accordance with prescribed procedures.

The CUI PM, in conjunction with the CUI SAO and OSY, shall recommend if sanctions to the offender are appropriate, or if other corrective action may be warranted (e.g., emphasis in training). Final determination to apply sanctions and the procedure for application of sanctions shall be in accordance with DAO 201-751, Discipline or bureau specific personnel management policies. Misuse of CUI that has been designated by another Executive bureau or agency shall be reported to that bureau or agency by the CUI PM of the offending organization.

37. SANCTIONS FOR MISUSE OF CUI [§ 2002.56]

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

When an individual is found to be responsible for the commission of a CUI incident, he/she may be subject to administrative, disciplinary, or criminal sanctions. The underlying law, regulation, or Government-wide policy is consulted to determine guidance on sanctions. The type of sanctions imposed is based on several considerations, including the following:

- Severity of the incident;
- Intent of the person committing the incident;
- Extent of training the person(s) has received;
- Prior acknowledgement of enterprise or system rules of behavior;
- Frequency of which the individual has been found responsible in the commission of other such incidents, to include Security Violations or Infractions involving classified information.

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

Administrative sanctions are assessed in accordance with the policies, procedures, and practices established by the Human Capital (personnel) office within the bureau, and actions involving the suspension or revocation of a security clearance are taken by the Office of Security in accordance with the applicable Executive Orders and Office of the Director of National Intelligence (ODNI) policies and regulations.

Where a proposed sanction associated with the unauthorized disclosure of CUI is greater than a reprimand, the bureau coordinates with the SAO, the Office of the General Counsel (OGC), and The Office of Security (OSY). Further, where a criminal violation has occurred that may result in a criminal prosecution, the matter is coordinated with the SAO and OGC and referred to the Department of Justice.

38. 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 Departmental Administrative Order 219-1, "Public Communications" and section 16 above.

CUI POCs, front line supervisors, and the Office of Public Affairs should routinely review DOC websites and social media sites to ensure that CUI is not posted.

39. REQUESTING NEW CATEGORIES OF CUI

Personnel who encounter information described in law, regulations, or government-wide policy that is not described in the CUI Registry must contact their CUI POC so that a new information category can be entered into the Registry.

The CUI POC shall coordinate the request through the programmatic 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,
- The name of the category applying to the information, and
- A suggested name, along with a suggested acronym for the category.

The CUI PM, in coordination with the Office of General Counsel, will submit the recommendation to NARA in accordance with the procedures contained in CUI Notice 2018-06: Establishing, Eliminating or Modifying Categories of Controlled Unclassified Information (CUI).