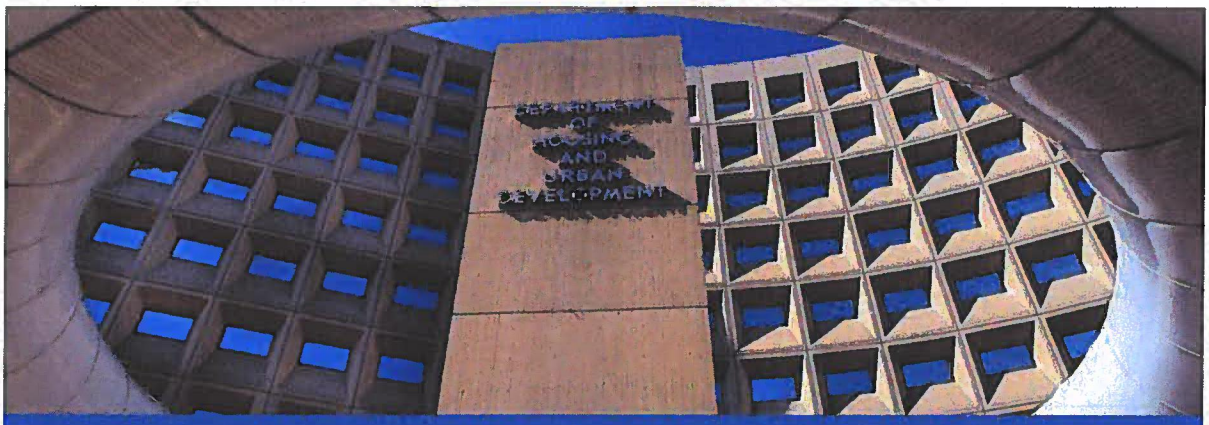


Controlled Information Program

Office of Emergency Management and National Security

6/16/25

1751.1 Version 1.0

Approval

Priscilla W. Clark
Chief Administrative Officer
Office of Chief Administrative Officer

NOTE: *This Handbook establishes procedures, program responsibilities, minimum standards, reporting protocols for the U.S. Department of Housing and Urban Development's (HUD) Controlled Information Program (CIP) for the protection of both controlled unclassified and classified national security information, assignment of responsibilities, and providing procedures for the designation, marking, protection, and the dissemination of said information. The guidance herein was developed primarily in accordance with Executive Order (EO) 13556, Controlled Unclassified Information, and EO 13526, Classified National Security Information. Combined, they form HUD's Controlled Information Program (CIP), defining responsibilities and procedures for HUD and must be applied accordingly.*

SCOPE: This Handbook applies to all HUD Offices, including Headquarters, Regions, Field Offices, and all other organizational entities within HUD, consultants, and contract employees.

PURPOSE: This Handbook sets forth the HUD policy, procedures, and framework for the general standards and safeguards to ensure protection of controlled information.

SUPERSESSION: This Handbook does not supersede or cancel any previous Handbook(s).

QUESTIONS: All questions or concerns regarding this Handbook must be submitted to CIP via CIP@hud.gov

EFFECTIVE DATE: This Handbook is approved and effective on the date of signature.

TABLE OF CONTENTS

Chapter 1: Overview **4**
Acronyms 4
Authorities and References 5
Responsibilities 5

Chapter 2: Controlled Unclassified Information **10**
Introduction 10
Authorities and References 10
Elements 11
Marking 11
Safeguarding 13
Dissemination and Reproduction 15
Decontrolling 17
Destruction 18
Handling 19
CUI Management 21
Disclosure Statutes 23

Chapter 3: Classified National Security Information **27**
Introduction 27
Authorities and References 27
Classification Management 27
Derivative Classification 31
Declassification 33
Classification Challenges 35
Reproduction 36
Safeguarding/Custody 37
Transmittal Documents 42
Receipt of Classified Information 44
Custody During Emergency 44
Information Systems and Network Security 45
Access Control 46
Foreign Government Information 47
Mail Processing Facility 48
Relocation 49
Destruction 49
Loss or Unauthorized Disclosure 50

Appendix A: Definitions **52**

Appendix B: CUI Marking Guide **61**

Appendix C: CNSI Marking Guide **65**

CHAPTER 1: OVERVIEW

ACRONYMS

ALJ	Administrative Law Judge
APA	Administrative Procedures Act
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CFR	Code of Federal Regulations
CIP	Controlled Information Program
CISO	Chief Information Security Officer
CNSI	Classified National Security Information
CPO	Chief Privacy Officer
CUI	Controlled Unclassified Information
DCA	Derivative Classification Authority
DOJ	Department of Justice
EA	Executive Agent
EOD	Entry-on-Duty
EO	Executive Order
ERA	Electronic Records Archives
FAR	Federal Acquisition Regulation
FIPS	Federal Information Processing Standards
FOIA	Freedom of Information Act
GAO	Government Accountability Office
GNMA	Government National Mortgage Association
GSA	General Services Administration
HUD	U.S. Department of Housing and Urban Development
IDE	Intrusion Detection Equipment
ISCAP	Interagency Security Classification Appeals Panel
ISOO	Information Security Oversight Office
NARA	National Archives and Records Administration
NATO	North Atlantic Treaty Organization
NISPOM	National Industrial Security Program Operating Manual
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSC	National Security Council
NSTISSI	National Security Telecommunications and Information System Security Instruction
OCA	Original Classification Authority
OEMNS	Office of Emergency Management and National Security
ODNI	Office of the Director of National Intelligence

OIG	Office of Inspector General
PSD	Personnel Security Division
PM	Program Manager
SAO	Senior Agency Official
SAP	Special Access Program
SCI	Sensitive Compartmented Information
SF	Standard Form
SPB	Security Policy Board
SSO	Special Security Officer
TR	Transfer Request
TSCM	Technical Surveillance Countermeasures

AUTHORITIES AND REFERENCES

A. See Chapter 2 for CUI
B. See Chapter 3 for CNSI

RESPONSIBILITIES

A. The Secretary, is responsible for delegating authority to the SAO for HUD's Intelligence and National Security Programs.

B. The SAO for Intelligence and National Security Programs, is responsible for:

1. Managing the CIP within HUD.

2. Ensuring that a PM is designated and dedicated resources are assigned to help manage the program.

3. Complying with all authorities and references for CUI and CNSI and this Handbook.

4. Ensuring all personnel comply with CUI and CNSI laws, regulations, and this Handbook.

5. Collaborating with the CISO and SAO for Privacy as necessary to ensure the protection, safeguarding, and dissemination of controlled information.

6. Providing the CIP PM's information to the EA both initially and when changes to the designation occur.

7. Reviewing and approving CUI and CNSI annual reports and assessments created by the CIP PM before being sent to the EA.

C. The Director, OEMNS, is responsible for:

1. Primary oversight of the CIP.

2. Identifying and designating the CIP PM in consultation with the SAO.

D. The CIP PM, is responsible for:

1. Coordinating all aspects of the day-to-day activities of the CIP and serving as the point of contact on all CUI and CNSI matters associated with the ISOO.

2. Establishing and maintaining procedures that will enable the prompt identification of any existing practice or condition that fails to afford adequate safeguarding of all controlled information in the possession of HUD or its contractors on its behalf and take prompt and effective action to correct any deficiency noted or reported.

3. Collaborating with the SSO, as needed, for the management of the CNSI Program pursuant to this Handbook and adhering to the delegated responsibilities outlined within the CNSI Chapter.

4. Adhering to the delegated responsibilities outlined within this Handbook.

5. Promulgating and publishing policies ensure procedures are established and implemented to prevent unauthorized and unnecessary access to controlled information.

6. Establishing and updating training programs and awareness materials for all personnel, including but not limited to mandatory EOD and annual refresher trainings.

7. Establishing and maintaining an ongoing HUD-wide self-inspection program, ensuring that CUI is handled, protected, disseminated, and destroyed in accordance with EO 13556.

8. Developing and maintaining processes to address improper or absent markings.

9. Establishing and maintaining the procedures and criteria for reporting and investigating misuse of CUI and CNSI.

10. Managing the CUI Program, to include:

a. Submitting to the EA, any law, regulation, or Government-wide policy not already incorporated into NARA's National CUI Registry that HUD proposes to use to designate unclassified information for safeguarding or dissemination controls.

b. Coordinating with the EA, 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.

c. Establishing processes for handling CUI decontrol requests submitted by authorized holders.

d. Providing within the CIP Annual Report, a description of all existing waivers along with the rationale for each waiver and, where applicable, the alternative steps being taken to ensure sufficient protection of CUI within HUD.

e. Establishing a mechanism by which authorized holders, both internal and external to HUD, can contact the designated PM for instructions when they receive unmarked or improperly marked information the agency designated as CUI.

f. Completing the Annual Data Collection Questionnaire as required by EO 13556.

11. Managing the CNSI Program, to include:

a. Establishing and maintaining procedures that will enable the prompt identification of any existing practice or condition that fails to afford adequate safeguarding of all classified information in the possession of HUD or contractors on behalf of HUD and take prompt and effective action to correct any deficiency noted.

b. Establishing and maintaining security education and training programs.

c. Establishing and maintaining an ongoing Department-wide CNSI self-inspection program.

d. Collaborating with PSD to ensure that CNSI related matters are addressed and resolved appropriately, when necessary.

e. Establishing procedures to prevent unnecessary access to classified information, that:

i. Require access to classified information be fully justified and established in writing before initiating administrative clearance procedures; and

ii. Ensure the number of individuals granted access to classified information is limited to the minimum consistent with operational and security requirements and needs.

f. Ensuring the performance plan(s) used to rate an employee's performance includes provisions regarding the management of classified information as a critical element or items to be evaluated in the rating of:

i. Security managers or security specialists, and

ii. All other personnel whose duties significantly involve the handling of classified information.

g. Accounting for the costs associated with classification-related activities.

h. Ensuring safeguarding practices are continually reviewed and eliminate those that are duplicative or unnecessary.

i. Promptly and fully investigating the circumstances of any violation, loss, or possible compromise of classified information including notifying the originating agency and coordinating any follow-up investigation or requests for information related to the incident.

j. Reviewing and approving or denying the modification or substitution of any standard procedures, specifications, or guidance set forth in this Handbook, based on a specific determination that such modification or substitution provides protection for classified information at least equal to that prescribed in EO 13526, ISOO Directive 1, and this Handbook.

E. The SSO, is responsible for:

1. Collaborating with the CIP PM, as needed, for the management of the CNSI Program pursuant to this Handbook.

2. Serving as the technical authority responsible for safeguarding SCI from unauthorized access or inadvertent disclosure by ensuring only duly authorized personnel with accredited need-to-know can access SCI.

3. Taking all appropriate action pertaining to the loss or possible compromise of classified information, including notifying the originating agency, ISOO, HUD OIG, and Federal law enforcement, if necessary.

4. Developing special contingency plans for the safeguarding of classified information used in or near hostile or potentially hostile areas.

5. Ensuring that all employees with access to classified information:

    a. Receive an initial security briefing on their security responsibilities and sign a Non-Disclosure Agreement before they are given access to classified information.

    b. Receive a debriefing, which will include a reminder of the criminal penalties related to unauthorized disclosure or classified information, when a need for access no longer exists or upon termination of employment, at which time they must also sign the debriefing portion of the NDA; and

    c. Receive refresher training on an annual basis to reinforce the policies, principles, and procedures that were provided in the initial briefing for access to classified information and any updates to those policies, principles, and procedures.

F. Employees and Contractors, are responsible for:

1. Complying with all CUI and CNSI laws, regulations, policies, and this Handbook.

2. Taking the mandatory training(s) within thirty (30) days of EOD and on an annual basis thereafter, and when appropriate or required.

CHAPTER 2: CONTROLLED UNCLASSIFIED INFORMATION

INTRODUCTION

CUI is one component within HUD's CIP, and this Chapter outlines the requirements for the handling, marking, protecting, sharing, destroying, disseminating, and decontrolling of CUI in accordance with the 32 CFR § 2002, as amended.

This Chapter is not intended to supersede or conflict with requirements outlined in the Privacy Act of 1974, as Amended (5 USC § 552a). When determining whether information must be protected under the Privacy Act, or whether the Privacy Act allows for the release of information to an individual, HUD will base its decision on the content of the information and the Privacy Act's criteria, regardless of whether the information has been marked as CUI. Any perceived conflicts with these policies should be addressed to the CIP PM, who will coordinate with the CPO to resolve any conflicts.

All HUD Offices and other organizational entities within HUD, except for GNMA, are required to implement management and control of CUI according to this Handbook. GNMA, for CUI policy purposes, may be regarded as an Agency in its own right, in accordance with 32 CFR § 2002.4(a), 5 USC § 105, and 12 USC § 1717(a)(2)(A), with the authority to develop and abide by its own CUI Policy in accordance with EO 13556 and 32 CFR § 2002.

AUTHORITIES AND REFERENCES

A. 5 U.S.C. Subchapter II, *Administrative Procedure Act*
B. 5 U.S.C. § 552a, *Records Maintained on Individuals, enacted by the Privacy Act of 1974 (P.L. 93 579*
C. 5 U.S.C. § 2302(b)(13) *Whistleblower Protection Act of 1989*
D. 5 U.S.C. § 3105, *Appointment of Administrative Law Judges, enacted by the Administrative Procedure Act*
E. 32 CFR § 2002, *Controlled Unclassified Information*, September 14, 2016
F. EO 13556, *Controlled Unclassified Information*, November 4, 2010
G. FAR 48 CFR Chapter 1
H. FAR 48 CFR § 52.204-21
I. Federal Information Security Management Act of 2002, as amended, 44 USC § 3541 et seq.
J. NARA CUI Notice 2017-01, *Implementation Recommendations for CUI Program*, June 12, 2019
K. NARA CUI Notice 2020-02, *Alternative Marking Methods*, June 3, 2020
L. NIST 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Lifecycle Approach for Security and Privacy*, December 2018
M. NIST Special Publication (SPP) 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*, September 2020 (includes updates as of Dec. 10, 2020)
N. NIST 800-60, Revision 2, *Guide for Mapping Types of Information and Systems to Security Categories*, January 31, 2014

O. NIST 800-88, Revision 1, *Guidelines for Media Sanitization*, December 2014
P. NIST 800-171, Revision 3, *Protecting CUI in Nonfederal Systems and Organizations,* May 2024
Q. NIST 800-171A, *Assessing Security Requirements for CUI*, May 2024
R. NIST Federal Information Processing Standards (FIPS) Publication (PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004
S. NIST FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006

ELEMENTS

A. HUD CUI Registry: Serves as the Department-wide repository for all information, guidance, policy, and requirements on handling CUI, including authorized CUI categories, associated markings, handling, and decontrolling procedures. This Registry will be maintained on the CIP intranet site.

B. Categories: All unclassified information that requires safeguarding or dissemination control must be handled within the parameters of this CUI Chapter and marked appropriately, per the guidance of this Handbook. Only records or materials that fall under the purview of the Categories may be marked as such and must be done in accordance with marking requirements. HUD may use only those Categories approved by the EA and published in the National CUI Registry (NARA CUI Registry) to designate information as CUI.

C. Types: There are two specific types of CUI encountered within the government:

1. CUI Basic is the subset of CUI for which the authorizing law, regulation, or Government-wide policy does not have any specific handling or dissemination requirements. CUI Basic is handled according to the uniform set of controls set forth in the CFR and the National CUI Registry.

2. CUI Specified does have specific handling and dissemination requirements. The National CUI Registry indicates which authorities include such specific requirements. CUI Specified controls may be more stringent than, or may simply differ from, those required by CUI Basic. CUI Specified is not a "higher level" of CUI, it is simply different. Since CUI Specified is based upon a law, federal regulation, or Government-wide policy, this form of CUI cannot be legally ignored or overlooked.

MARKING

A. All CUI documents must be marked and protected according to applicable laws, regulations, and Government-wide policies. For purposes of HUD, it has been designated that "Controlled Unclassified Information", "CUI", or "Controlled" are the official markings authorized to designate unclassified information requiring safeguarding or dissemination controls. All HUD

personnel, which includes employees, contractors, and consultants, shall be prohibited from using all other markings or practices not included in this Chapter. If legacy markings remain, they immediately become voided and no longer indicate that the information is protected or that it is or qualifies as CUI.

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

C. When it is impractical to individually mark CUI due to quantity or nature of the information, or when HUD 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 including NARA-approved coversheet, user access agreements, computer system encryption, digital privacy screens, or signs in storage areas, and in containers.

D. The lack of a CUI marking on information that qualifies as CUI does not exempt the authorized holder from abiding by applicable CUI marking and handling requirements as described in this Handbook and the National CUI Registry. Any incorrectly marked document should be brought to the attention of CIP@hud.gov immediately.

E. Working Papers: Working papers containing CUI must be marked and protected during the draft phase(s) the same as the finished product, and as required for any CUI contained within them. This applies whether or not the working papers will be shortly destroyed. When the working papers are no longer needed, they should be destroyed as described in the "Destruction of CUI" section of this Handbook.

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

For additional information on Marking CUI, refer to Appendix B: CUI Marking Guide.

SAFEGUARDING

A. Pursuant to EO 13556, the CUI EA issues safeguarding standards and, as necessary, updates them as needed. These standards require HUD to safeguard CUI at all times, in a manner that minimizes the risk of unauthorized disclosure while allowing timely access by authorized holders.

B. The objective of safeguarding is to prevent the unauthorized disclosure of, or access to CUI. All personnel must adhere to the following general safeguarding policies:

1. CUI, regardless of its form, must be protected in a manner that minimizes the risk of unauthorized disclosure while allowing for access by authorized holders.

2. Safeguarding measures that HUD is authorized or accredited to use for classified information and national security systems are also sufficient for safeguarding CUI in accordance with HUD's management and acceptance of risk.

3. All controlled information should be protected even if the markings are incorrect or missing. Due to varied time spans of agencies transitioning from legacy markings to CUI, some controlled information may not be marked properly or may not be marked at all. This information should still be treated and safeguarded as CUI. Anyone finding an incorrectly marked document should notify the CIP PM via CIP@hud.gov.

4. Safeguarding During Working Hours: Personnel working with CUI shall be careful not to expose CUI to others who do not have a lawful government purpose to see it. For further protection, cover sheets (e.g., SF 901, SF 902, and SF 903) should be used to conceal their contents from casual viewing. Personnel should 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.

5. Unless different protection is specified in the National 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.

6. HUD may increase CUI Basic's confidentiality impact level above moderate only internally, or by means of agreements with other agencies, or non-executive branch entities (including agreements for the operation of an information system on behalf of HUD).

7. HUD may not require controls for CUI Basic at a level higher than permitted in the CUI Basic requirements when disseminating the CUI Basic outside of HUD.

8. Authorized holders within HUD must comply with the policy in EO 13556, and complete the Department-wide CUI training, as well as the applicable regulations in 32 CFR § 2002, this Handbook, and the National CUI Registry. For information designated as CUI Specified, authorized holders must also follow the procedures in the underlying laws, regulations, or Government-wide policies.

9. Other Precautions

    a. Personnel shall reasonably ensure that unauthorized individuals cannot access or observe CUI, or overhear conversations where CUI is being discussed;

    b. CUI must 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;

    c. When outside 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 casual observation; and,

    d. Personnel must protect the confidentiality of CUI that is processed, stored, or transmitted on federal information systems in accordance with applicable policy or procedure.

C. Care While Traveling: CUI shall not be viewed while on public transportation where others may be exposed to it. In hotel rooms, CUI must 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.

D. Shipping or Mailing: When shipping or mailing CUI, authorized holders:

1. May use the United States Postal Service or any commercial delivery service that offers in-transit automated tracking and accountability tools. However, as of September 30, 2022, under the *Social Security Fraud Protection Act of 2017*, full social security numbers of individuals may not be sent through the mail, unless the HUD Secretary has determined that the inclusion of the social security number is necessary.

2. Shall use in-transit automated tracking and accountability.

3. May use interoffice or interagency mail systems to transport CUI.

4. Address packages 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.

E. CUI Within Information Systems: HUD must protect the confidentiality of CUI processed, stored, or transmitted on federal information systems in accordance with the applicable security requirements and controls established in FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems*, FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems*, and NIST SPs 800–53, *Security and Privacy Controls for Federal Information Systems*, and 800-60, *Guide for Mapping Types of Information and Systems to Security Categories and Organizations*.

1. HUD OCIO may increase the confidentiality impact level for CUI Basic above moderate only within HUD, including contractors operating an information system on behalf of HUD, or by means of agreements between HUD and other agencies. HUD 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 HUD.

2. Personnel may not treat non-federal information systems as though they are HUD systems, so non-executive branch entities cannot be required to protect these systems in the same manner that HUD might protect its own information systems. 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.

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

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

DISSEMINATION AND REPRODUCTION

A. Access or dissemination of CUI may only occur provided the sharing of CUI:

1. Abides by the laws, regulations, or Government-wide policies that established the CUI category;

2. Furthers a lawful Government purpose;

3. Is not restricted by an authorized limited dissemination control established by the CUI EA; and

4. Is not otherwise prohibited by law.

B. Non-Executive Branch or Foreign Entity: CUI may be shared with a non-executive branch or a foreign entity under the following conditions in addition to the requirements listed above:

1. 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.

2. Whenever feasible, some type of formal information-sharing agreement with the recipient of the CUI must be in place. The agreement must include a requirement for the recipient to, at a minimum, comply with EO 13556; 32 CFR § 2002; and the National CUI Registry.

3. Information-sharing agreements that were made prior to the establishment of CIP should be updated whenever feasible so they do not conflict with CIP requirements.

4. 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 HUD is not the designating agency, personnel must report any non-compliance to the designating agency.

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

a. HUD must use CUI markings rather than alternative ones for safeguarding or dissemination controls on CUI received from or sent to foreign individuals; and,

b. Such foreign individuals must abide by any requirements set by the CUI category or sub-category's governing laws, regulations, or Government-wide policies, etc.

C. CUI Basic may be disseminated to individuals and entities meeting the access requirements of this section. Authorized recipients of CUI Basic may further disseminate the information to individuals or entities, thereby meeting and complying with the requirements of this CUI policy.

D. Limited Dissemination of CUI: Only the limited dissemination controls published in the National 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 this Handbook, and significant doubt still remains, please consult with the designated CIP PM at CIP@hud.gov for further guidance.

1. 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.

2. In the absence of specific dissemination restrictions in the authorizing law, regulation, or Government-wide policy, HUD may disseminate CUI Specified as it would CUI Basic.

E. Reproduction of CUI: CUI may be reproduced (e.g., copied, scanned, printed, or otherwise 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, HUD personnel 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 drive or memory is sanitized in accordance with NIST SP 800-88.

DECONTROLLING

A. CUI shall be decontrolled when an authorized holder, consistent with the HUD CUI Registry, removes safeguarding or dissemination controls from CUI that no longer require such controls. Authorized holders may decontrol as soon as practicable any CUI designated by HUD that no longer requires safeguarding or dissemination controls, unless doing so, conflicts with the

governing law, regulation, or Government-wide policy. The following are other scenarios in which CUI may be decontrolled:

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

2. When HUD or other agencies disclose it in accordance with an applicable information access statute, such as the FOIA or the Privacy Act (when legally permissible), provided the designator's agency incorporates such disclosures into its public release processes;

    a. Disclosures under FOIA constitute CUI decontrol for all purposes; or

    b. 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).

    c. 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.

3. 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; or

4. A predetermined event or date specified by HUD occurs, or as described under Handling in Section C, unless law, regulation, or Government-wide policy requires coordination first.

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

C. The authorized holder must clearly indicate that decontrolled CUI is no longer controlled when restating, paraphrasing, reusing, releasing to the public, or donating CUI to a private institution. Line through or remove the CUI markings to indicate it is no longer being controlled as CUI.

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

DESTRUCTION

A. Authorized users may destroy CUI when:

1. HUD no longer needs the information; and

2. Records disposition schedules published or approved by NARA allow.

B. When destruction of CUI is required, the HUD Form 1067, *Records Destruction Form*, must be completed with approved authorization. Upon completion, HUD Form 1067-A, *Certificate of Sanitization*, must also be completed.

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

1. 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 CUI Notice 2017-02: *CUI and Multi-Step Destruction Process*.

2. Any method of destruction approved for CNSI, as delineated in 32 CFR § 2001.47, Destruction, or any implementing or successor guidance.

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

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

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

HANDLING

A. Transmittal/ Transporting: When a transmittal document accompanies CUI, the transmittal document must include a CUI marking on its face, indicating that CUI is attached or enclosed. The

transmittal document must also include noticeably on its face the following or similar instructions, as appropriate:

1. HUD no longer needs the information; and when the transmittal document is removed, this document is Uncontrolled Unclassified Information; or

2. Upon removal of the transmittal document, the document does not contain CUI.

3. CUI may be sent through the United States Postal Service or any commercial delivery service that offers in-transit automated tracking and accountability tools.

4. CUI may also be sent through the interoffice or interagency mail systems.

5. 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.

B. Transferring Records To NARA: When feasible, HUD must decontrol records containing CUI prior to transferring them to NARA. When decontrolling records is not feasible prior to transferring them to NARA, HUD must:

1. Indicate on the TR in NARA's ERA or on the SF-258 records 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 § 1235, § 1250, § 1256); and

2. For hard copy transfer, do not place a CUI marking on the outside of the container.

3. If HUD does not indicate the status as CUI on the TR or SF-258, NARA may assume that HUD decontrolled the information prior to transfer, regardless of any CUI markings on the actual records.

C. Commingling of CUI with CNSI: When authorized holders include CUI in documents that also contain CNSI, the decontrolling provisions of EO 13556 and this Handbook apply only to portions marked as CUI. In addition, authorized holders must:

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

2. Include the CUI control marking, CUI category and subcategory markings, and limited dissemination control markings in an overall banner marking.

CUI MANAGEMENT

A. Training: HUD personnel who have access to CUI must receive initial training within 30 days of employment and at least once every year thereafter. This CUI policy delineates the specifics of mandatory training. Advanced CUI Training is also available and may be mandatory for those who create, own, and/or use CUI regularly.

B. Misuse and Incident Reporting

1. When CUI is used in a manner not in accordance with this policy contained in EO 13556, this Handbook, the HUD CUI Registry, or the applicable laws, regulations, and Government-wide policies that govern the affected information, it is considered misuse. Misuse 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.

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

    b. All employees, contractors and lessors must report suspected or confirmed misuse of CUI or other CUI related violations to the CIP PM at CIP@hud.gov immediately.

    c. Where laws, regulations, or Government-wide policies governing certain categories of CUI specifically establish sanctions for the misuse of CUI, agencies are responsible for coordinating with the appropriate parties concerning sanctions.

C. Reportable CUI incidents

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

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

3. Any incident involving computer, 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.

4. 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.

5. 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.

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

7. Any incident in which CUI is inadvertently revealed to or released to a person who is not authorized access.

8. Any incident in which CUI has been destroyed by unauthorized means.

9. Any incident in which CUI has been reproduced without authorization or contrary to specific restrictions imposed by the originator.

10. Any incident in which CUI has been shared contrary to an applied dissemination control marking.

11. Any other incident in which CUI is not safeguarded or handled in accordance with prescribed procedures.

D. Sanction for Misuse of CUI: Consequences for misuse of CUI are based on existing HUD policies and the type of information involved (building information, PII, etc.). Each policy's applicable consequences shall apply. Consequences may incur disciplinary action in accordance with HUD policy.

E. Challenges To CUI Designation

1. Authorized holders of CUI who, in good faith, believe that its designation as CUI is improper or incorrect, or who believe they have received unmarked CUI, should notify the disseminating agency of this belief. When HUD is not the designating agency, the authorized holder must notify the designating agency.

2. If the information at issue is involved in Government litigation, or the challenge to its designation or marking as CUI arises as part of the litigation, the issue of whether the challenger may access the information will be addressed via the litigation process instead of by HUD's CIP.

3. Challengers should notify the CIP PM of the issue.

F. Waivers: HUD has not requested any CUI-related waivers. If a need arises to obtain a waiver, it may be granted when it is impractical to individually mark CUI due to quantity or nature of the information (e.g., forms, blueprints, etc.). Contact the CIP PM by emailing CIP@hud.gov if you believe a CUI waiver is required.

G. Self-Inspection: In accordance with 32 CFR § 2002, HUD must maintain internal oversight efforts to measure and monitor implementation and management of the CUI Program within CIP. The CIP PM, under the authority of the CUI SAO, shall provide technical guidance, training, and materials for HUD components to conduct reviews and assessments of their CUI Programs at least annually, and to report the results to the CIP PM as NARA requires. The Self-Inspection Program includes:

1. Following training of the designated CIP PM, they shall conduct annual self-inspections of HUD's CUI within CIP and report the results on a schedule determined by the CUI SAO. The CIP PM 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; and

2. Following guidance and inspection materials received from the CIP 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.

3. The CIP PM shall:

    a. Provide the components formats for documenting self-inspections; and

    b. Recording findings and provide advice for resolving deficiencies and taking corrective actions.

    c. Results from the Department-wide self-inspections shall include updates to the CUI training provided to HUD personnel.

DISCLOSURE STATUTES

A. The fact that HUD designates certain information as CUI does not affect HUD determinations pursuant to any law which requires HUD or the employee to disclose that information or permits them to do so as a matter of discretion. HUD or the employee must make such determinations according to the criteria set out in the governing law, not based on the information's status as CUI. CUI does not override the requirements of existing disclosure statutes. Disclosure determinations must be based on the applicable law, regulation, or Government-wide policy and not the information's status as CUI.

B. Agreement Content: All agreements with non-executive branch entities going forward must include, at a minimum, provisions that state:

1. Non-executive branch personnel entities must handle CUI in accordance with EO 13556, the regulations in 32 CFR § 2002, this Handbook, and the HUD CUI Registry;

2. Misuse of CUI is subject to penalties established in applicable laws, regulations, or Government-wide policies; and

3. The non-executive branch personnel must report any non-compliance with handling requirements to HUD via the CIP email: CIP@hud.gov

4. Non-disclosure forms and agreements must include the anti-gag provision as required by law 5 U.S.C. § 2302(b)(13)); and

5. Confidentiality clauses in personnel settlement agreements must include the anti-gag provision if the clause restricts disclosure of any other information beyond the terms and conditions of the agreement itself.

C. When HUD is not the agency that designated or approved the designation of a specific item of information as CUI (i.e., the designating agency), the agency that disseminated the item (i.e., the disseminating agency) to HUD must notify HUD of any non-compliance with handling requirements.

D. Pre-existing Agreements: All current information sharing agreements, entered into prior to July 1, 2025, must be updated to address any terms in the agreement that conflict with the requirements in EO 13556, the National CUI Registry, and this Handbook when feasible.

E. Exceptions to Agreements

1. HUD need not enter into a written agreement when CUI is shared with the following bodies:

a. Congress, including any committee, subcommittee, joint committee, joint subcommittee, or office thereof; or

b. A court of competent jurisdiction, or any individual or entity when directed by an order of a court of competent jurisdiction or a Federal ALJ appointed under the U.S. Constitution Article. II, § 2, clause 2 and the *Administrative Procedure Act*, 5 U.S.C. § 3105; or

c. The Comptroller General, in the course of performing duties of the Government Accountability Office; or

d. Individuals or entities, when HUD releases information to them pursuant to a FOIA or Privacy Act request.

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

G. If a HUD Office or Region determines that, despite public disclosure of the CUI through FOIA, there is still an identifiable need to continue to protect the information as CUI within the Department, then the HUD Office or Region must consult with the CIP PM and OGC.

H. CUI and the *Whistleblower Protection Act*

1. This policy does not change or affect existing legal protections for whistleblowers. The fact that HUD designates or marks certain information 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, or executive order or directive.

2. These provisions are consistent with and do not supersede, conflict with, or otherwise alter individuals' obligations, rights, or liabilities created by existing statute or EO relating to (1) classified information, (2) communications to Congress, (3) the reporting to an Inspector General or the Office of Special Counsel of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, or (4) any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by controlling Executive Orders and statutory provisions are incorporated into this policy and are controlling.

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

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

CHAPTER 3: CLASSIFIED NATIONAL SECURITY INFORMATION

INTRODUCTION

Information that has been determined, pursuant to EO 13526, *Classified National Security Information*, or any predecessor order, to require protection against unauthorized disclosure, shall be classified, marked, safeguarded, and declassified in accordance with the requirements of the EO 13526.

HUD shall not determine original classification for information and does not have an OCA. HUD directors and officials specifically identified by position may have access to CNSI received from other agencies.

The protection of classified information, including but not limited to, CNSI is the responsibility of individuals who possess knowledge of such information, regardless of how the information is obtained. All HUD managers, supervisors, employees, consultants, and contract employees with access to CNSI must handle and safeguard this classified information in accordance with the requirements of EO 13526, 32 CFR § 2001, and this Handbook.

AUTHORITIES AND REFERENCES

A. EO 12829, *National Industrial Security Program* (January 6, 1993)
B. EO 12968, *Access to Classified Information* (August 2, 1995)
C. EO 13526, *Classified National Security Information* (December 29, 2009)
D. EO 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information* (October 7, 2011)
E. 32 CFR § 2001, *Classified National Security Information*
F. 32 CFR § 2004, *National Industrial Security Program (NISP)*

CLASSIFICATION MANAGEMENT

A. Original Classification

1. OCA is limited by EO 13526 to agencies that have demonstrated a need for classification authority. HUD does not have OCA.

2. In exceptional cases, when an employee or contractor at HUD originates information they believe requires classification, the information will be protected in a manner consistent with this Handbook. If information is created within HUD which the originator feels needs to be classified, the SSO must be immediately contacted for assistance. The information must be transmitted promptly to the agency that has appropriate subject matter interest and classification authority with respect to the information. This agency has 30 days to decide

whether to classify the information. Complete guidance for original classification can be found in ISOO Directive 1.

3. If it is not clear which agency has classification responsibility for the information, it must be sent by registered mail (at no time will information believed to be classified be sent electronically within or outside of HUD) to the Director of ISOO. The Director of ISOO will determine which agency has primary subject matter interest and forward the information, with appropriate recommendations, to the agency for classification.

B. Classification Levels: Classification levels provide context of and support to proper safeguarding and handling of classified information. Except as otherwise provided by statute, no other terms are used to identify U.S. classified information. Further, these terms are not to be used or applied to unclassified information that does not meet the standards for classification in accordance with this Handbook and EO 13526. Information may be classified at one of the following three levels:

1. **TOP SECRET** - Applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the OCA is able to identify or describe; or

2. **SECRET** - Applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the OCA is able to identify or describe; or

3. **CONFIDENTIAL** - Applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the OCA is able to identify or describe.

C. Classification Prohibitions: Information is not classified to:

1. Conceal violations of law, inefficiency, or administrative error; or

2. Prevent embarrassment to a person, organization, or agency; or

3. Restrain competition; or

4. Prevent and/or delay the release of information not requiring protection in the interest of national security; or

D. Basic scientific information not clearly related to national security shall not be classified.

E. Marking Prohibitions: Do not use other terms, such as “Official Use Only”, “Sensitive But Unclassified,” “Limited Official Use,” “Sensitive Security Information,” “Administratively Confidential,” or “Controlled Unclassified Information” to identify classified information. The aforementioned terms are or have been (in the past) utilized as categories to describe handling procedures for unclassified sensitive information, and not as a classification of material under EO 13526.

F. Training: All authorized HUD personnel who create, process or handle classified information must undergo training to ensure a satisfactory knowledge and understanding about classification, safeguarding, and declassification policies and procedures.

1. Initial Training: All cleared HUD personnel shall receive initial training on basic security policies, principles, practices, criminal, civil, and administrative penalties. Such training must be provided in conjunction with the granting of security clearance, and prior to granting access to classified information.

2. Specialized security education and training: Original classification authorities, authorized declassification authorities, individuals specifically designated as responsible for derivative classification, classification management officers, security managers, security specialists, and all other personnel whose duties significantly involve the creation or handling of classified information should receive more detailed training. This training should be provided before or concurrent with the date the employee assumes any of the positions listed above, but in any event no later than six months from that date.

3. Refresher security education and training: Refresher training shall be provided to employees who create, process or handle classified information. Refresher training should reinforce the policies, principles, and procedures covered in initial and specialized training. Refresher training should also address issues or concerns identified during HUD’s self-inspections.

4. Termination briefings: HUD should ensure that each employee granted access to classified information who leaves the service of the Department receives a termination briefing. Also, each HUD personnel whose clearance is withdrawn must receive such a briefing. At a minimum, the termination briefing should impress upon each individual:

    a. His or her continuing responsibility not to disclose any classified information to which the employee had access and the potential penalties for noncompliance; and

    b. The obligation to return to the SSO all classified documents and materials in the individual’s possession.

5. Other security education and training: HUD may develop additional security education and training when deemed necessary.

G. Self-Inspection: HUD is required to establish and maintain an ongoing self-inspection program, which must include the regular reviews of the agency's derivative classification actions and shall authorize an appropriate agency official to correct misclassification actions in accordance with section 5.4(d)(4) of EO 13526 and 32 CFR 2001.60(c)(2).

Enforcement of HUD policy requires the periodic internal review and evaluation of personnel activities with respect to the effective implementation of the classified information program as established under EO 13526. These standards are binding and apply to all offices that process, handle, and/or store classified information, equipment, or materials, including contractors pursuant to NISPOM described in EO 12829. An annual report of the Department's self-inspection program may be provided to the Director of the Information Security Oversight Office.

NISPOM prescribes the security requirements, restrictions, and safeguards applicable to private industry under U.S. Government contract, including contractor-conducted self-inspections. The standards in NISPOM are consistent with the standards prescribed in EO 13526.

1. Inspection Procedures and Frequency: Inspections and frequency are based on program needs and the magnitude of security activity. The CIP PM should conduct at least one inspection of classified storage containers and their contents annually. An inspection summary and out-briefing must be provided to the individual responsible for the inspected container following the inspection.

2. Elements of an Inspection: The elements of the security inspection include, but are not limited to, the elements noted below. The scope of the self-inspection may expand according to program or policy needs.

3. A review of relevant security directives, guides, and instructions.

4. Interviews with key personnel, derivative classifiers, users, and/or holders of classified materials concerning their understanding of security responsibilities and requirements.

5. A review of access and control records.

6. A review of internal procedures and processes pertaining to the protection, control, and safeguarding of classified information.

7. A review of SECRET materials, and/or a review of TOP SECRET materials.

8. Safeguarding: The review will include determining compliance with the following items:

    a. Adherence to established standards for safeguarding classified information;

    b. Compliance with controls for access to classified information;

    c. Assessment of effectiveness of the information security program in detecting and processing security violations and preventing recurrences; and

    d. Assessment of compliance with the procedures for identifying, reporting, and processing unauthorized disclosures of classified information.

9. Evaluating the effectiveness of procedures to ensure that:

    a. The CIP PM exercises proper control over the classified information it generates, processes, handles, and/or stores;

    b. Holders of classified information do not disclose information originated by another agency without that agency's authorization, except in emergency situations; and

    c. Departing or transferring individuals with access to classified information return all classified information in their possession to their designated classified information custodian, prior to termination of security clearance.

DERIVATIVE CLASSIFICATION

A. Information classified derivatively on the basis or source documents, or classification guides must bear all markings prescribed below. When using a classified source document as the basis for derivative classification, the markings on the source document determine the markings to be applied to the derivative document.

1. DCA is tied to an individual or position that has an official need to derivatively classify. Before being authorized to derivatively classify, individuals are identified, trained, and certified based on the following, established HUD standards:

    a. Identification: The individuals or positions that have a need to derivatively classify material must be identified.

b. Training: Each Derivative Classifier must receive initial training, as well as refresher training at least once every two (2) years, in order to retain their DCA.

c. Certification: Before a Derivative Classifier is certified, they must complete the required training to demonstrate that they are aware of proper derivative classification procedures and markings.

2. Derivative Classification Authority Identity: Derivative classifiers shall be identified by name and position, or by personal identifier, in a manner that is immediately apparent on each derivatively classified document. If not otherwise evident, the agency and office of origin shall be identified as follows the name on the "Classified by" line. Must appear as:

   Classified by: "Frances Jones, Lead Analyst, Research and Analysis Division" or

   Classified by: ID# IMN01

B. Derivative Classification Application

1. The Derivative Classifier must observe and respect original classification decisions; and carry forward to any newly created documents the pertinent classification markings.

2. The Derivative Classifier must use only authorized sources to make derivative classification decisions, including classification guidance, memorandums, or other formal documents issued by an OCA;

3. The Derivative Classifier must explicitly and uniformly apply classification and control markings when creating, disseminating, or using classified HUD information to maximize information sharing while protecting sources, methods, and activities from unauthorized or unintentional disclosure;

4. The Derivative Classifier must determine appropriate classification markings for the HUD information that they produce, and apply appropriate control markings that correctly implement DoD and ODNI guidelines for dissemination; and

5. Portion-mark all HUD documents that contain HUD information requiring control markings, regardless of classification, format, or medium in accordance with applicable DoD and ODNI standards.

C. Derivative Classification Marking: Markings shall be applied according to the requirements of EO 13526, 32 CFR § 2001, and ISOO Booklet: *Marking Classified National Security Information,*

Revision 4 (January 2018). Implementation must be in accordance with this Handbook, see Appendix D: CNSI Markings.

Classification markings cited on the source or in a security classification guide must be respected and carried forward to the newly created document.

D. Derivative Classification Records

1. Individuals performing derivative classification actions must maintain a record of each action taken. For derivatively classified documents, the record should include the total number of derivatively classified documents, delineated by classification level.

2. Records should be maintained by fiscal year and submitted to Chief/Deputy Chief, ODMNS as part of annual reporting requirements.

3. Records of classification actions must be counted and reported by document (not by page).

DECLASSIFICATION

A. HUD shall cooperate with NARA in managing automatic declassification of accessioned federal records, presidential papers and records, and donated historical materials under the control of the Archivist of the United States.

Information should remain classified as long as it is in the best interest of national security to keep it protected, and continued classification is in accordance with the requirements of EO 13526.

If an employee has reason to believe that the public interest in disclosure of information outweighs the need for continued classification, they will refer the matter to the appropriate OCA or the SSO for an assessment and determination on whether declassification is appropriate.

B. Automatic Declassification

1. Automatic Declassification at Twenty-Five (25) Years

a. Automatic Declassification of Permanent Historical Records. EO 13526, Section 3.3, Automatic Declassification, mandates that information contained within permanently valuable historical records (as defined by USC Title 44, *Disposal of Records*) be automatically declassified twenty-five (25) years from the date of origin of the document. All classified records are automatically declassified on December 31 of the year that is

twenty-five (25) years from the date of origin, except where such information has been exempted from automatic declassification at twenty-five (25) years.

2. Onset of Automatic Declassification. The following provisions apply to the onset of automatic declassification:

   a. Classified records within an integral file block that are otherwise subject to automatic declassification under this section, are not automatically declassified until December 31 of the year that is 25 years from the date of the most recent record within the file block. For the purposes of automatic declassification, integrated file blocks contain only records dated within ten years of the file block.

   b. In consultation with the Director of the National Declassification Center, before the records are subject to automatic declassification, the Secretary or the HUD SAO may delay automatic declassification for up to five (5) additional years for classified information contained in microforms, motion pictures, audiotapes, videotapes, or comparable media that make a review for possible declassification exemptions more difficult or costly.

   c. By notification to the Director, ISOO, the Secretary or HUD SAO may delay automatic declassification for up to 90 days from the date of discovery of classified records that were inadvertently not reviewed prior to the effective date of automatic declassification.

C. Mandatory Declassification Review

1. Any individual, except those identified in paragraph 4 below, may request a review for declassification of information classified under EO 13526, or its predecessor orders. Such requests must be sent to HUD's Office of Government Information Management or the SAO for Privacy (or successor office).

2. Declassification does not apply to any request for a review made to an element of the intelligence community that is requested by a person other than a U.S. citizen, legal permanent resident, foreign government entity, or representative thereof.

3. Documents required to be submitted as part of a prepublication review or other administrative process pursuant to an approved non-disclosure agreement are not covered by this section.

4. Information originated by the incumbent President, the incumbent President's White House Staff, committees, commissions, or boards appointed by the incumbent President, or other entities within the Executive Office of the President that solely advise and assist the incumbent President, are exempt from the provisions of this Section.

CLASSIFICATION CHALLENGES

A. In circumstances where authorized holders of classified information, who, in good faith, believe the classification status is improper, may challenge the classification status of the information. Classification challenges are presented to the Classifier of the information. Challenges may be received from any authorized holder of the information, to include HUD employees, contractors, employees and contractors of other Federal Agencies, or State, local, tribal, and private sector partners.

NOTE: Where necessary, assistance and/or anonymity in processing a classification challenge can be obtained by processing the challenge through the SSO.

1. Formal Classification Challenges: Formal challenges to classification must be submitted in writing and presented to the SSO who will then forward the challenge to the OCA and notify the CIP PM.

    a. For each type of challenge, the following applies:

        i. Unclassified. Must take every precaution to ensure it remains unclassified.

        ii. Classified. Must be marked and safeguarded accordingly.

    b. All correspondence must sufficiently describe the information being challenged and briefly explain why the information should not be classified at a particular level other than its current level in the source document.

    c. Individuals submitting a classification challenge will not be subject to retribution for bringing such actions. SSO honors a challenger's request for anonymity and serves as the agent for the challenger in processing the challenge.

    d. The individual submitting the challenge has a right to appeal the decision to the ISCAP established by EO 13526, Section 5.3, *Interagency Security Classification Appeals Panel*.

    e. Challenged information will remain classified and is protected at its highest level of classification until a final classification determination is made by the appropriate OCA, and/or the ISCAP.

2. Informal Classification Challenges: The classification challenge provision does not prohibit an authorized holder from informally questioning the classification of information through direct and informal contact with the classifier. When appropriate, or when uncertainties exist over the classification status, holders of classified information are encouraged to make direct contact with the classifier to obtain clarification. When a change in classification results from an informal challenge, the challenger will ensure the Official from whom the change was received is authorized to make such a change, and a record of the change, to include the Official's name, position, Agency, and date is maintained with a file copy of the document. The OCA making the decision is responsible for notifying holders of the change in classification.

REPRODUCTION

A. Information Reproduction of classified material must be limited to those instances when it is absolutely necessary. CONFIDENTIAL and SECRET information may be reproduced without prior approval of the originator unless otherwise indicated on the document. When TOP SECRET or SECRET material is reproduced, the additional copies must be recorded on the SECRET or TOP SECRET Classified Document Control Log forms. Reproduction of TOP SECRET material requires coordination with the originator and the TOP SECRET Control Officer. During reproduction, the following copier security procedures must be followed:

1. Cleared individuals must remain at the copier until classified reproduction is complete;

2. Digital copiers with electronic chip memory capabilities must be utilized only in a stand-alone capacity. Digital copiers used to reproduce classified information must be connected to any network or telephone line;

3. Before leaving the copier, individuals must check the copier for any copies or originals that may be left in the copier;

4. Classified waste, such a rejected copier or blank copies run after classified material is processed, must be destroyed in a cross-cut shredder approved for the destruction of classified information;

5. If the copier malfunctions and the copier cannot be cleared or the copies cannot be retrieved, the SSO must be contacted to ensure that the copier is removed from service until it can be ascertained that the malfunction has been properly cleared; and

6. No unescorted maintenance person will be allowed access to any reproduction equipment used for the reproduction of classified materials.

SAFEGUARDING/CUSTODY

A. Protection: Classified information, regardless of its form, must be afforded a level of protection against loss or unauthorized disclosure commensurate with its level of classification and under conditions designed to deter and detect unauthorized access to the information:

1. Ensures that evidence of tampering can be detected;

2. Precludes inadvertent access; and

3. Provides a method which assures timely delivery to the intended recipient.

B. Transmitting: Individuals transmitting classified information are responsible for ensuring that intended recipients are authorized individuals with the capability to store classified information in accordance with this Handbook. All classified information physically transmitted outside facilities must be enclosed in two layers, both of which provide reasonable evidence of tampering, and which conceal the contents. The inner enclosure should clearly identify the address of both the sender and the intended recipient, the highest classification level of the contents, and any appropriate warning notices. The outer enclosure should be the same except that no markings indicate that the contents are classified should be visible. Intended recipients must be identified by name only as part of an attention line. The following exceptions apply:

1. If the classified information is an internal component of a packable item of equipment, the outside shell or body may be considered as the inner enclosure provided it does not reveal classified information;

2. If the classified information is an inaccessible internal component of a bulky item of equipment, the outside or body of the item may be a sufficient enclosure provided observation of it does not reveal classified information;

3. If the classified information is an item of equipment that is not reasonably packable and the shell or body is classified, it should be concealed with an opaque enclosure that will hide all classified features;

4. Specialized shipping containers, including closed cargo transporters or diplomatic pouch, may be considered the outer enclosure when used; and

5. When classified information is hand-carried outside a facility, a locked briefcase may serve as the outer enclosure.

C. Transmittal: Couriers and authorized individuals designated to hand-carry classified information must ensure that the information remains under their constant and continuous protection and that direct point-to-point delivery is made. As an exception, agency heads may approve, as a substitute for a courier on direct flights, the use of specialized shipping containers that are of sufficient construction to provide evidence of forced entry, are secured with a high security padlock, are equipped with an electronic seal that would provide evidence of surreptitious entry and are handled by the carrier in a manner to ensure that the container is protected until its delivery is completed.

D. Storage: Classified information must be stored only under conditions designed to deter and detect unauthorized access to the information.

1. Requirements for Physical Protection

a. "TOP SECRET" information must be stored in GSA approved security container with the following supplemental control:

i. An Intrusion Detection system (IDS) with the personnel responding to the alarm arriving within fifteen (15) minutes of the alarm annunciation; or

ii. Acceptability of IDE: All IDE must be UL-listed (or equivalent as defined by the SSO) and approved by the SSO. Government and proprietary installed, maintained, or furnished systems are subject to approval only by the SSO.

b. "SECRET" information must be stored by one of the following methods:

i. In the same manner as prescribed for "TOP SECRET" information; or

ii. In a GSA-approved security container without supplemental controls

c. "CONFIDENTIAL" information must be stored in the same manner as prescribed for "TOP SECRET" and "SECRET"; and

d. Supplemental Controls: Admittance to any area where classified information is stored must be limited to authorized personnel. Individuals who are not authorized access, but whose presence in the area is temporarily required, must be escorted and kept under constant observation. All classified information must be covered or otherwise protected from observation, disclosure, or removal.

e. Combinations

i. Equipment in Service: The classification of the combination must be the same as the highest level of classified information that is protected by the lock. Combinations to dial-type locks must be changed only by persons having a favorable determination of eligibility for access to classified information and authorized access to the level of information protected unless other sufficient controls exist to prevent access to the lock or knowledge of the combination. Combinations must be changed under the following conditions:

1. Whenever such equipment is placed into use;

2. Whenever a person who knows the combination no longer requires access to it, unless other sufficient controls exist to prevent access to the lock; or

3. Whenever a combination has been subject to possible unauthorized disclosure.

ii. Equipment Out of Service

1. When security equipment is taken out of service, it must be inspected to ensure that no classified information remains and the built-in combination lock must be reset to a standard combination (50-25-50); and

2. Safe and Combination Records: Combinations to security equipment containing classified information must be recorded on an SF700, *Security Container Information*. Each part of the SF700 must be completed in its entirety. The names, addresses and home telephone numbers of personnel responsible for the combination, and the classified information therein, must be indicated on Part 1 of the SF700. The completed Part 1 must be posted in the front interior of the top control or locking drawer of the security equipment. Part 2 must be inserted in a Part 2A envelope provided and forwarded via secure means to the SSO. Also, Part 2 must have the highest level of classified information stored in the security container annotated in the top border area of the completed SF700.

2. Each GSA approved container used for the storage of classified information is required to have an SF702, *Security Container Check Sheet* attached to the outside, where it is clearly visible, on which an authorized person will record the person responsible, after-hours contact number, date, and actual time each business day that they initially unlock and finally lock the security container, followed by their initials.

3. Requirements for Physical Protection

    a. GSA approved security containers used for the storage of classified information that have been opened on a particular day must not be left unattended until they have been locked by an authorized person and checked by a second person. In the event that a second person is not available within the office, the individual who locked the container must annotate the "Checked by" column of the SF702. When all spaces are completed, the Form must be affixed to the container in plain view, to be available for after-hours inspections and upon request during periodic inspections conducted by the SSO.

    b. A reversible "OPEN-CLOSED" or "LOCKED-UNLOCKED" placard must also be used on such security equipment. The respective side of the sign must be displayed to indicate when the container is open or closed.

        NOTE: GSA approved containers are intended for the storage of classified information.

    c. Classified information must not be stored with:

        i. Firearms/ammunition;

        ii. Money; or

        iii. Personal items such as purses, radios, or jewelry.

4. Repairing Security Containers

    a. Persons who repair or drill security containers and locks must be cleared for access to the highest level of classified information stored within the container, or must be escorted and continuously watched while working on the container.

    b. Although repaired containers cannot be used to store TOP SECRET information, GSA-approved containers can be returned to their original state of security for storage up to the SECRET level by meeting the following conditions;

    c. All damaged or altered parts must be repaired;

    d. When a container is drilled adjacent to or through the dial ring, the lock must be replaced with a computerized combination lock meeting Federal Specification FF-L-2740. The drilled hole must be repaired with a tapered casehardened steel rod (dowel, drill it, bearing) with a diameter and length slightly larger than the hole. When the rod is driven

into the hole, a shallow recess should remain at each end of the rod that is no less than one-eighth inch or 3.175 mm, or more than three-sixteenths inch or 4.76 mm deep. This will permit a substantial weld on the inside and outside surfaces. The outside of the drawer head must then be puttied, sanded, and repainted in such a way that no visible evidence of the hole or its repair remains on the outer surface after replacement of the damaged parts; and

e. Containers that have been drilled or repaired in a manner other than that described above cannot be restored to their original state of security integrity. The "Test Certification Label" and the "GSA Approved Security Container" label, if any, must be removed. The container must not be used for storing classified information and a notice to this effect must be marked on the front of the container.

5. Information Controls

a. Combinations must be committed to memory and not annotated anywhere other than on the SF700, *Security Container Information*.

b. When selecting a combination to be set on a security container do not use the following numbers:

i. Standard manufacturer's settings of 50-25-50;

ii. Zero, or numbers between 0 and 20, for the last number of the combination (a common source of lock malfunction);

iii. Numbers in straight ascending or descending order, such as 29-37-51 or 51-37-29;

iv. Numbers ending in 5 or 0 (e.g., 35, 60, etc.); or

v. Numbers derived from birthdates, addresses, telephone numbers, etc.

c. The processing of classified information on non-classified HUD information systems is prohibited.

d. Classified document cover sheets alert personnel that documents or folders are classified and require protection from unauthorized scrutiny. Individuals who prepare or package classified documents are responsible for affixing the appropriate document cover sheet. Colors; orange "TOP SECRET" cover sheet (SF703); red "SECRET" cover sheet (SF704); and blue "CONFIDENTIAL" cover sheet (SF705), are the only authorized cover sheets for

collateral classified information. Document cover sheets must be used to shield classified documents while in use and particularly when the transmission is made internally. File folders containing classified information must be marked at the top and bottom of the front and back covers to indicate the overall classification of the contents rather than permanently affixing the respective classified document cover sheet.

TRANSMITTAL DOCUMENTS

A. Classified information must be transmitted and received in an authorized manner that ensures that evidence of tampering can be detected, and that inadvertent access can be precluded. Persons transmitting classified information are responsible for ensuring that intended recipients are authorized persons with the capability to store classified information in accordance with this Handbook.

   Classified information to be transmitted outside of an HUD facility must be enclosed in opaque inner and outer covers.

   1. The inner cover must be a sealed wrapper or envelope plainly marked with the assigned classification and addresses of both sender and addressee;

   2. The outer cover must be sealed and addressed, with no indication of the classification of its contents; and

   3. A receipt must be attached to or enclosed in the inner cover. CONFIDENTIAL information requires a receipt only if the sender deems it necessary.

      a. The receipt must identify the sender, the addressee and the document, but contain no classified information; and

      b. The receipt must be immediately signed by the recipient and returned to the sender.

B. The transmittal of TOP SECRET information of a HUD facility must be carried out by:

   1. Specifically authorized personnel; or

   2. State Department diplomatic pouch; or

   3. Messenger-courier system authorized for that purpose, for example:

      a. The Defense Courier Service; or

b. Over authorized secure communications circuits.

4. Under no circumstances should TOP SECRET information be transmitted via the U.S. Postal Service.

C. The transmittal of SECRET information among the 50 States, the District of Columbia, and Commonwealth of Puerto Rico should be by one of the means authorized for TOP SECRET information; by the U.S. Postal Service registered mail or express mail service; or by protective services provided by U.S. air or surface commercial carriers under such conditions as may be prescribed by the SSO. The use of streetside mail collection boxes or commercial building hallway drop shafts is strictly prohibited;

D. CONFIDENTIAL information must be transmitted within and between the 50 States, the District of Columbia, the Commonwealth of Puerto Rico, and U.S. territories by means established for higher classifications: or by the U.S. Postal Service's certified mail. Outside these areas, CONFIDENTIAL information will be transmitted only as is authorized for higher classifications. However, CONFIDENTIAL information must not be transmitted to government contractor facilities via U.S. Postal Service First Class Mail. When first class mail is used, the envelope or outer wrapper must be marked to indicate that the information is not to be forwarded but is to be returned to sender. The use of streetside mail collection boxes or commercial building hallway drop shafts is prohibited; and

E. Hard carrying of classified information in travel status

1. If it is determined that the transportation of classified information by an individual in travel status is in the best interest of the U.S. Government, the following specific safeguards will apply:

a. Classified information must be in the physical possession of the individual and must always have adequate safeguards if proper storage at a U.S. Government facility is not available. Under no circumstances should classified information be stored in a hotel safe or room, locked in train or bus station lockers, automobiles, private residences, train compartments, or any vehicular detachable storage compartments;

b. An inventory of all classified information, including cable messages, must be made prior to departure and a copy of same must be retained by the traveler's office until the traveler's return, at which time all classified information must be accounted for;

c. Classified information must never be displayed or used in any manner in public conveyances or rooms. Travelers are responsible for reviewing and familiarizing

themselves with required classified materials, under appropriate secure circumstances, in advance of their travel and not during travel;

d. To avoid unnecessary delays in the screening process prior to boarding commercial air carriers, the traveler must have in his or her possession written authorization from the SSO to transport classified information;

e. Upon completion of the visit, the traveler must have all classified information being returned to his or her office by approved means. All TOP SECRET or SECRET classified information, including cable messages transported for the purpose of the visit, must be accounted for. It is highly recommended that the traveler also account for CONFIDENTIAL information. If the traveler is delivering or transferring any TOP SECRET or SECRET classified items to another office, the traveler must obtain a signed receipt; and

f. When transporting classified information, any HUD employee or contractor must have in his or her possession an official courier *pro tem* letter signed by the SSO, or his or her designated official.

Receipt of Classified Information

A. Custodian of classified information at the level of TOP SECRET must use the HUD Form 1447, *Classified Document Receipt* to:

1. Register an accurate, unclassified description of each document, its assigned control number, date of receipt, classification, and disposition; and,

2. Record all changes in status or custody of the document during the period it is retained.

B. Forward a current inventory of all classified documents to the SSO at the end of each fiscal year, using the HUD Form 1448, *Document Control Register Log*.

Custody During Emergency

A. In the event of fire, natural disaster, civil disturbance, or an evacuation of office space, classified information must be protected by placing it in locked storage cabinets or safes, or by proper destruction. Individuals who are away from their offices and have classified information in their possession at the time must properly safeguard such information.

B. In emergency situations where there is an imminent threat to life, or in defense of the homeland, the SSO may authorize the disclosure of classified information to an individual or individuals who are otherwise not routinely eligible for access. In such cases, the following conditions will apply:

1. The amount of classified information disclosed must be kept to the absolute minimum to achieve the purpose.

2. Individuals who receive classified information must be limited.

3. The classified information must be transmitted via approval of Federal Government channels by the most secure and expeditious method, or other means deemed necessary when time is of the essence.

4. Instructions must be provided to the recipients about what specific information is classified, how it will be safeguarded, and that it must remain in the physical custody of an authorized Federal Government entity in all but the most extraordinary of circumstances.

5. Recipients must be appropriately briefed on their responsibilities not to disclose the information and they must sign a nondisclosure agreement.

6. Within 72 hours of disclosure of classified information, or at the earliest opportunity the emergency permits, but no later than 30 days after the release, the SSO will provide the originating agency the following information:

    a. A description of the disclosed information;

    b. To whom the information was disclosed;

    c. How the information was disclosed and transmitted;

    d. Reason for the emergency release;

    e. How the information is being safeguarded; and

    f. A description of the briefings provided and a copy of the nondisclosure agreements signed.

INFORMATION SYSTEMS AND NETWORK SECURITY

A. Classified information electronically accessed, processed, stored, or transmitted must be protected in accordance with applicable national policy issuances identified in the *Index of NSTISSI and Director of Central Intelligence Directive 6/3*. The requirement for technical countermeasures such as TSCM and TEMPEST necessary to detect or deter exploitation of classified information through technical collection methods must be determined and HUD may

apply countermeasures in accordance with NSTISSI 7000, *Tempest Countermeasures for Facilities*, and SPB Issuance 6-97, *National Policy on Technical Surveillance Countermeasures*.

1. 32 CFR 2001.50, *Telecommunications Automated Information Systems and Network Security*:

    a. Electronic communication of classified information over regular fax machine, telephone or computerized communications equipment is prohibited.

    b. Transmission of classified information will only be via encrypted methods. This means use of a secure encrypted telephone, fax machine, or other properly encrypted communications device.

    c. Federal telecommunications security policies are developed and issued under the purview of the NSC. Implementing instructions are issued by the NSA. Processing classified information on a laptop (unless approved by the SSO), handheld device, or desktop computer or via a HUD computer network is prohibited.

    d. Processing classified information must only be done on a laptop computer that has been approved by the SSO for processing classified information.

ACCESS CONTROL

A. A system of control measures must be maintained to ensure that access to classified information is limited to only authorized individuals. The control measures must be appropriate to the environment in which access occurs and the nature and volume of the information. The system should include technical, physical, and personnel control measures. Administrative control measures which may include records of internal distribution, access, generation, inventory, reproduction, and disposition of classified information must be required when technical, physical, and personnel control measures are insufficient to deter and detect access by unauthorized persons.

1. Reproduction: Reproduction of classified information must be held to the minimum consistent with operational requirements. The following additional control measures must be taken:

    a. Reproduction must be accomplished by authorized persons knowledgeable of the procedures for classified reproduction;

    b. Unless restricted by the OCA, TOP SECRET, SECRET, and CONFIDENTIAL information may be reproduced to the extent required by operational needs, or to facilitate review for declassification;

c. Copies of classified information should be subject to the same controls as the original information; and

d. The use of technology that prevents, discourages, or detects the unauthorized reproduction of classified information is encouraged.

FOREIGN GOVERNMENT INFORMATION

A. The requirements described below are additional baseline safeguarding standards that may be necessary for the foreign government information, other than NATO information, that requires protection pursuant to an existing treaty, agreement, bilateral exchange or other obligation.

1. Storage: Foreign government information must be stored separately from other classified information. This may be accomplished by utilizing separate storage drawers of a container.

2. Safeguarding Standards

a. TOP SECRET

i. Records must be maintained of the receipt, internal distribution, destruction, access, reproduction, and transmittal of foreign government TOP SECRET information. Reproduction requires the consent of the originating government.

ii. Destruction must be witnessed.

b. SECRET

i. Records must be maintained of the receipt, external dispatch and destruction of foreign government SECRET information.

ii. Other records may be necessary if required by the originator. SECRET foreign government information may be reproduced to meet mission requirements unless prohibited by the originator. Reproduction must be recorded unless the originator waives this requirement.

c. CONFIDENTIAL: It is not necessary to maintain records for foreign government CONFIDENTIAL information unless otherwise required by the originator.

d. Restricted and other foreign government information provided in confidence: To assure the protection of other foreign government information provided in confidence (e.g.,

foreign government "Restricted," "Designated," or unclassified provided in confidence), such information must be classified under EO 13526. HUD employees and/or contractor, acting in accordance with instructions received from the U.S. Government, must provide a degree of protection to the foreign government information at least equivalent to that required by the government or international organization that provided the information. When adequate to achieve equivalency, these standards may be less restrictive than the safeguarding standards that ordinarily apply to U.S. CONFIDENTIAL information. If the foreign protection requirement is lower than the protection required for U.S. CONFIDENTIAL information, the following requirements must be met:

i. Documents can retain their original foreign markings if the SSO, or designated official, determines that these marking are adequate to meet the purpose served by U.S. classification markings. Otherwise, documents marked, "This document contains (insert name of country) (insert classification level) information to be treated as (insert classification level)." The notation, "Modified Handling Authorized," may be added to either foreign or U.S. markings authorized for foreign government information. If re-marking foreign originated documents or matter is impractical, an approved cover sheet is an authorized option;

ii. Documents will be provided only to those who have an established need-to-know, and where access is required by official duties;

iii. Individuals being given access must be notified of applicable handling instructions. This may be accomplished by providing a briefing, written instructions, or by applying specific handling requirements to an approved cover sheet;

iv. Documents must be stored in such a manner so as to prevent unauthorized access;

v. Documents must be transmitted in a method approved for classified information, unless the origination government waives this requirement; and

vi. Third-country transfer. The release or disclosure of foreign government information to any third-country entity must have the prior consent of the originating government if required by a treaty, agreement, bilateral exchange, or other obligation.

MAIL PROCESSING FACILITY

A. The supervisor of a mailroom must develop procedures to protect classified information that may be contained in incoming mail, bulk shipments, or items delivered by messenger.

B. All incoming mail, bulk shipments, and items delivered by messenger must be forwarded directly to the individual addressed on the envelope.

RELOCATION

A. When classified information is physically moved from one office or facility to another, it must be retained in a locked, approved security container. Supervisors or program managers responsible for control of the security container must notify the SSO, prior to relocating a security container, so the security officer can note the new location of the container in the facility security inventory.

B. The custodian or other cleared personnel must maintain constant supervision of the container during the move. The custodian is responsible for notifying the SSO of the new location of the container. The custodian must also annotate any changes to the relocation of the security container on the SF700, Security Container Information form.

DESTRUCTION

A. Classified information identified for destruction must be destroyed completely to preclude recognition or reconstruction of the classified information in accordance with procedures and methods prescribed by HUD.

1. Custodians of classified information who have classified information identified for destruction must destroy the information completely by a National Security Agency (NSA) approved crosscut document shredder to preclude recognition or reconstruction. Records of the destruction of each TOP SECRET or SECRET classified document must be kept. The HUD Form 1450, *Classified Document Destruction Certificate* must be completed, dated and signed at the time of destruction, by two witnesses for TOP SECRET information and one witness for SECRET information. A copy of the destruction record must be maintained for a minimum of five years in accordance with *General Records Schedule 4.2 Item 040* (Records of Accounting for and Controlling Access to Records).

2. Technical guidance concerning appropriate methods, equipment, and standards for the destruction of classified electronic media and processing equipment components may be obtained by submitting all pertinent information to the National Security Agency/Central Security Service, Directorate for Information Systems Security, Fort Meade, MD 20755. Specifications concerning appropriate equipment and standards for the destruction of other physical storage media may be obtained from GSA.

LOSS OR UNAUTHORIZED DISCLOSURE

A. Any person with knowledge that classified information has been lost, or may have been lost, possibly compromised, or disclosed to an unauthorized person(s), must telephonically report the circumstances immediately to the CIP PM, or designated official to the address shown below:

CIP Program Manager
U.S. Department of Housing and Urban Development
451 7th Street SW
Washington, DC 20410

B. Cases involving information originated by a foreign government or another U.S. Government agency. HUD must notify the other Government agency or foreign government of the circumstances and findings that affect their information or interests. However, foreign governments normally must not be advised of any security system vulnerabilities that contributed to the compromise.

C. An inquiry or investigation will be conducted by CIP PM, or the OIG, and upon adjudicating the matter, the appropriate office will recommend remedial and/or disciplinary legal actions.

D. Corrective actions for security violations

1. Any individual, at any level of employment, determined to be responsible for the loss, unauthorized release or disclosure or potential release or disclosure of classified information, whether it be knowingly, willfully or through negligence, will be notified in writing that his or her action is in violation of this Handbook, and EO 13526, and that he or she is subject to administrative or legal actions;

2. Repeated failure, neglect or disregard of established requirements for safeguarding classified information by any HUD employee or contractor cleared for access to classified information, will be grounds for appropriate adverse or disciplinary action. Such actions include, but are not necessarily limited to, a letter or warning, a letter of reprimand, suspension without pay, or dismissal, as appropriate in the particular case, under applicable personnel rules, regulations and procedures. Where a violation of criminal statutes may be involved, any such case will be promptly referred to the Office of Inspector General, or the Department of Justice; and,

3. As the occasion demands, reports of security violations will be placed in the employee's personnel security file, and as appropriate, in the employee's official personnel folder.

Note: Section 5.5 of EO 13526 requires that HUD notify the Director of the ISOO when a violation under paragraphs (b)(1), (2) or (3) of this section occurs.

APPENDIX A: DEFINITIONS

1. Access: The ability or opportunity to come into possession of controlled information.

2. Agency: Any ‘‘executive agency,’’ as defined in 5 USC 105; the United States Postal Service; and any other independent entity within the executive branch that designates or handles CUI.

3. Agreements and Arrangements: Any vehicle that sets out 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, HUD should enter into written agreements or arrangements that include CUI provisions whenever feasible. When sharing information with foreign entities, HUD should enter agreements or arrangements when feasible.

4. Authorized holder: An individual, agency, organization, or group of users that is permitted to designate or handle CUI, in accordance with 32 CFR § 2002.

5. Authorized person: A person who has a favorable determination of eligibility for access to classified information, has signed an approved nondisclosure agreement, SF-312, *Classified Information Nondisclosure Agreement,* or the agency specified nondisclosure agreement and has a need-to-know for the specific classified information in the performance of official duties.

6. Classification: The act or process by which information is determined to be classified.

7. Classified information: Any information or material that has been determined by the Government pursuant to an Executive Order, statute, or regulation, to require protection against unauthorized disclosure for reasons of national security.

8. CNSI (or classified information): Information that has been determined pursuant to EO 13526, or any predecessor order or successor order, to require protection against unauthorized disclosure and is marked to indicate its classified status when in document form.

9. CONFIDENTIAL Source: Any individual or organization that has provided, or that may reasonably be expected to provide, information to the US on matters pertaining to national security with the expectations that the information or relationship or both, as to be held in confidence.

10. Control level: A general term that indicates the safeguarding and disseminating requirements associated with CUI Basic and CUI Specified.

11. Controlled environment: 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.

12. Controlled Unclassified Information (CUI): 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. However, CUI does not include classified information or information a nonexecutive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency.

13. Controls: Safeguarding or dissemination controls that a law, regulation, or Government-wide policy requires or permits HUD to use when handling CUI. The authority may specify the controls it requires or permits HUD to apply, or the authority may generally require or permit agencies to control the information (in which case, the agency applies controls from EO 13556, 32 CFR § 2002, and the National CUI Registry).

14. CUI Basic: The subset of CUI for which the authorizing law, regulation, or Government-wide policy does not set out specific handling or dissemination controls. HUD handles CUI Basic according to the uniform set of controls set forth in 32 CFR § 2002 and the National 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.

15. CUI categories: Types of information for which laws, regulations, or Government-wide policies require or permit HUD to exercise safeguarding or dissemination controls, and which the CUI EA has approved and listed in the National CUI Registry. The controls for any CUI Basic categories and any CUI Basic subcategories are the same, but the controls for CUI Specified categories and subcategories can differ from CUI Basic ones and from each other. A CUI category may be Specified, while some or all of its subcategories may not be, and vice versa.

16. CUI Category Markings: Markings approved by the CUI EA for the categories and subcategories listed in the National CUI Registry.

17. CUI Executive Agent (EA): The National Archives and Records Administration (NARA), which implements the executive branch-wide CUI program and oversees Federal agency actions to

comply with EO 13556. NARA has delegated this authority to the Director of the Information Security Oversight Office (ISOO).

18. CUI Program: The executive branch-wide program to standardize CUI handling by all Federal agencies. The Program includes the rules, organization, and procedures for CUI, established by EO 13556, 32 CFR § 2002, and the National CUI Registry.

19. CUI Program Manager: An agency official, designated by the agency head or CUI SAO, to serve as the official representative to the CUI EA on HUD's day-today CUI program operations, both within the agency and in interagency contexts.

20. CUI Registry: The online repository for all information, guidance, policy, and requirements on handling CUI, including everything issued by the CUI EA other than 32 CFR § 2002. 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.

21. CUI Senior Agency Official (SAO): A senior official designated in writing by an agency head and responsible to that agency head for implementation of the CUI program within that agency. The CUI SAO is the primary point of contact for official correspondence, accountability reporting, and other matters of record between the agency and the CUI EA.

22. CUI Specified: The subset of CUI in which the authorizing law, regulation, or Government-wide policy contains specific handling controls that it requires or permits agencies, such as HUD, to use that differ from those for CUI Basic. The National 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.

23. Damage to National Security: Harm to the national defense, domestic and abroad, or foreign relations of the US, resulting from the unauthorized disclosure of information. Aspects of the information, such as its sensitivity, value, utility, and provenance of the information must be taken into consideration.

24. Declassification: The authorized change in the status of information from classified information to unclassified information.

25. Declassification Authority: (i) The official who authorized the original classification, if that official is still serving in that position; (ii) The originator's current successor in function; (iii) a supervisory official of either; or (iv) officials delegated declassification authority in writing by the agency head or the SAO.

26. Decontrolling: Occurs when an authorized holder, consistent with 32 CFR § 2002 and the National CUI Registry, removes safeguarding or dissemination controls from CUI that no longer require such controls. Decontrolling CUI may occur automatically or through agency action.

27. Derivative Classification: The incorporating, paraphrasing, restating, or generating in new form information that is already classified and marking the newly developed material consistent with the classifications marking that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

28. Designating CUI: Occurs when an authorized holder, consistent 32 CFR § 2002 and the National CUI Registry, determines that a specific item of information falls into a CUI category or subcategory. The authorized holder who designates the CUI must make recipients aware of the information's CUI status in accordance with 32 CFR § 2002.

29. Designating Agency: The executive branch agency that designates or approves the designation of a specific item of information as CUI.

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

31. Document: Any tangible thing which constitutes or contains information and is the original and any copies (whether different from the originals because of notes made on such copies or otherwise) of all writings of every kind and description over which an agency has authority. Document encompasses materials inscribed by hand or by mechanical, facsimile, electronic, magnetic, microfilm, photographic, or other means, as well as phonic or visual reproductions or oral statements, conversations, or events, and including, but not limited to: correspondence, email, notes, reports, papers, files, manuals, books, pamphlets, periodicals, letters, memoranda, notations, messages, telegrams, cables, facsimiles, records, studies, working papers, accounting papers, contracts, licenses, certificates, grants, agreements, computer disks, computer tapes, telephone logs, computer mail, computer printouts, worksheets, sent or received communications of any kind, teletype messages, agreements, diary entries, calendars and journals, printouts, drafts, tables, compilations, tabulations, recommendations, accounts, work papers, summaries, address books, other records and recordings or transcriptions of conferences, meetings, visits, interviews, discussions, or telephone conversations, charts,

graphs, indexes, tapes, minutes, contracts, leases, invoices, records of purchase or sale correspondence, electronic or other transcription of taping of personal conversations or conferences, and any written, printed, typed, punched, taped, filmed, or graphic matter however produced or reproduced. Documents also include the file, folder, exhibits, and containers, the labels on them, and any metadata, associated with each original or copy. In addition, documents include voice records, film, tapes, video tapes, email, personal computer files, electronic matter, and other data compilations from which information can be obtained, including materials used in data processing.

32. Federal Information System: An information system used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. 44 USC 3554(a)(1)(A)(ii).

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

34. Foreign Government Information: (i) Information provided to the US Government by a foreign government or governments, an international organization, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence; (ii) information produced by the US Government pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or (iii) information received and treated as “foreign government information” under the terms of a predecessor order.

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

36. Holders: Authorized persons who have access to classified information.

37. Infraction: Any knowing, willful, or negligent action contrary to the requirements of EO 13526, 32 CFR § 2001, EO 13556, 32 CFR § 2002, or this HUD Handbook.

38. Integrity: The state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed.

39. Lawful Government purpose: 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).

40. Legacy Material: Unclassified information that an agency marked as restricted from access or dissemination in some way, or otherwise controlled, prior to the CUI program.

41. Limited Dissemination Control: Any CUI EA-approved control that agencies may use to limit or specify CUI dissemination.

42. Mandatory Declassification Review: The review for declassification of classified information in response to a request for declassification that meets the requirements under section 3.5 of EO 13526.

43. Misuse of CUI: Occurs when someone uses CUI in a manner not in accordance with the policy contained in EO 13556, 32 CFR § 2002, the National CUI Registry, HUD 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.

44. National Institute of Standards and Technology (NIST): A research institute within the U.S. Department of Commerce that promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology.

45. National Security: The national defense of foreign relations of the United States.

46. National Security System: A special type of information system (including telecommunications systems) whose function, operation, or use is defined in National Security Directive 42, *National Policy for the Security of National Security Telecommunications and Information Systems*, and 44 USC 3542(b)(2).

47. Need-to-Know: A determination within the executive branch in accordance with directives issued pursuant to EO 13526 that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

48. Network: A system or two or more computers that can exchange data or information.

49. Non-Executive Branch Entity: A person or organization established, operated, and controlled by individual(s) acting outside the scope of any official capacity as officers, employees, or agents of the executive branch of the Federal Government. Such entities may include elements of the legislative or judicial branches of the Federal Government; State, interstate, tribal, or local government elements; and private organizations. A nonexecutive branch entity does not include foreign entities as defined in 32 CFR § 2002, nor does it include individuals or organizations

when they receive CUI information pursuant to Federal disclosure laws, including the Freedom of Information Act (FOIA) and the Privacy Act of 1974

50. On behalf of an agency: Occurs when a non-executive branch entity uses or operates an information system or maintains or collects information for the purpose of processing, storing, or transmitting Federal information, and those activities are not incidental to providing a service or product to the Government.

51. Order: Executive Order 13556 *Controlled Unclassified Information*, November 4, 2010 (3 CFR, 2011 Comp., p. 267), Executive Order 13526 *Classified National Security Information*, December 29, 2009 or any successor orders.

52. Original Classification: An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure.

53. Original Classification Authority (OCA): An individual authorized in writing, either by the President, the Vice President, or by agency heads or other officials designated by the President, to classify information in the first instance.

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

55. Principal Office: The primary location where an agency's leadership directs, controls, or coordinates the agency's activities.

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

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

58. Records: Agency records and Presidential papers or Presidential (or Vice Presidential) records, as those terms are defined in 44 USC 3301 and 44 USC 2201 and 2207. Records also include such items created or maintained by a Government contractor, licensee, certificate holder, or

grantee that are subject to the sponsoring agency's control under the terms of the entity's agreement with the agency.

59. Required or Permitted (by law, regulation, or Government-wide policy): The basis by which information may qualify as CUI. If a law, regulation, or Government-wide policy requires that agencies, such as HUD, exercise safeguarding or dissemination controls over certain information, or specifically permits agencies, such as HUD, the discretion to do so, then that information qualifies as CUI. The term 'specifically permits' in this context can include language such as ''is exempt from'' applying certain information release or disclosure requirements, ''may'' release or disclose the information, ''may not be required to'' release or disclose the information, ''is responsible for protecting'' the information, and similar specific but indirect, forms of granting the agency discretion regarding safeguarding or dissemination controls. This does not include general agency or agency head authority and discretion to make decisions, risk assessments, or other broad agency authorities, discretions, and powers, regardless of the source. The National CUI Registry reflects all appropriate authorizing authorities.

60. Re-Use: Incorporating, restating, or paraphrasing information from its originally designated form into a newly created document.

61. Self-Inspection: The internal review and evaluation of individual HUD activities, and HUD, as a whole, with respect to the implementation of the program established under EO 13556, 32 CFR § 2002, 13526 and 32 CFR § 2001.

62. Senior Agency Official (SAO): The official designated by the Secretary under section 5.4(d) of EO 13526 to direct and administer HUD's program under which information is classified, safeguarded, and declassified.

63. Sensitive Compartmented Information (SCI): Information about certain intelligence sources and methods and can include information pertaining to sensitive collection systems, analytical processing, and targeting, or which is derived from it.

64. Special Access Program (SAP): Means a program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.

65. Special Security Officer (SSO): Responsible for management of HUD Sensitive Compartmented Information (SCI) programs. SCI and/or Special Access Program (SAP) mission requirements shall be coordinated with the SSO by the operating unit identifying the access need.

66. Source Document: An existing document that contains originally classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

67. Telecommunications: The preparation, transmission, or communication of information by electronic means.

68. Unauthorized Disclosure: A communication or physical transfer of controlled information to an unauthorized recipient.

69. Uncontrolled Unclassified Information: Information that neither EO 13556 nor the authorities governing classified information cover as protected. Although this information is not controlled or classified, agencies, such as HUD, must still handle it in accordance with the Federal Information Security Modernization Act (FISMA of 2014), FOIA, and Privacy Act of 1974 requirements.

70. Violation: (i) Any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information; (ii) Any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of EO 13526, or its implementing directive, or (iii) Any knowing, willful, or negligent action to create or continue a special access program contrary to the requirements of EO 13526.

71. Working Papers: Documents or materials, regardless of form, that an agency or user expects to revise prior to creating a finished product.

APPENDIX B: CUI MARKING GUIDE

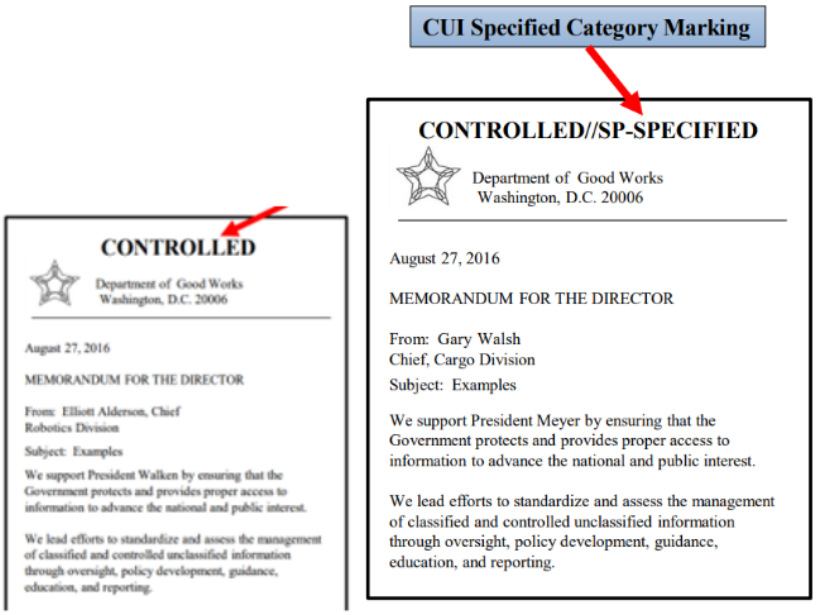
Markings which were applied prior to the start of the CUI Program, and are inconsistent with the CUI markings, are considered legacy markings (e.g., For Official Use Only, Agency Internal Use Only). Information with legacy markings that is not shared outside of the Agency does not need to be remarked with CUI markings. However, if an authorized holder is using legacy information or information derived from a legacy document that qualifies as CUI in a new document, the new document must contain CUI markings and follow proper CUI safeguarding and handling guidelines.

A. CUI Banner Marking: The primary marking for all CUI is the CUI Banner Marking. This is the main marking that appears at the top of each page of any document that contains CUI.

   1. This marking is MANDATORY for all documents containing CUI.

   2. The content of the CUI Banner Marking must be inclusive of all CUI within the document and must be the same on each page.

   3. The Banner Marking should appear as bold capitalized black text and be centered when feasible.



NOTE: Once you begin marking a document every page in the document must also be marked.

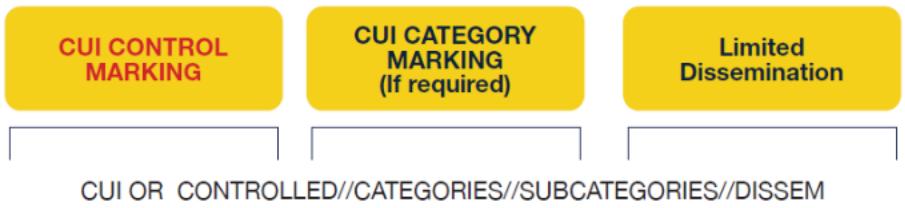
4. The CUI Banner Marking may include up to three elements:

   a. The industry standard for CUI Banner Marking is "**CUI**" though "**CONTROLLED UNCLASSIFIED INFORMATION**" and "**CONTROLLED**" are also acceptable.

   b. CUI Category or Subcategory Markings (mandatory for CUI Specified): These are separated from the CUI Control Marking by a double forward slash (//). When including multiple categories or subcategories in a Banner Marking, they must be alphabetized and are separated by a single forward slash (/).

   c. Limited Dissemination Control Markings: These are preceded by a double forward slash (//) to separate them from the rest of the CUI Banner Marking.

      Here is an example:



      NOTE: The above example uses the words "CATEGORIES" and "SUBCATEGORIES" as substitutes for CUI Category or Subcategory Markings and the word "DISSEM" as a substitute for a Limited Dissemination Control Marking. Consult the National CUI Registry for actual CUI markings.

B. Designation Indicator

   1. All documents containing CUI must indicate the agency of designation (a letterhead, signature block, or "Controlled By" line) on the first page or cover of all documents containing CUI.

   2. Include the contact information of the designating agency and identify a point of contact or division within the organization.

C. CUI Portion Marking: Portion marking of CUI is optional in a fully unclassified document but is permitted and encouraged to facilitate information sharing and proper handling of the information. As determined by OCA, HUD is approved to use CUI Portion Marking. When CUI Portion Marking is used, these rules must be followed:

1. CUI Portion Markings are placed at the beginning of the portion to which they apply and must be used throughout the entire document.

2. CUI Portion Markings are contained within parentheses and may include up to three elements:

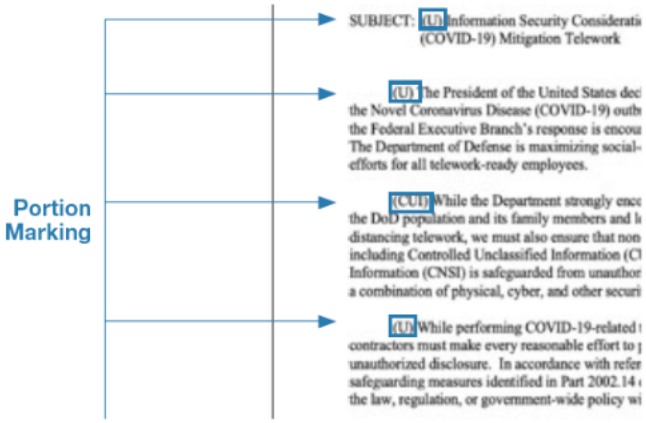
    a. The CUI Control Marking: This is mandatory when portion marking and must be the acronym “CUI” (the word “Controlled” will not be used in portion marking).

    b. CUI Category or Subcategory Markings: These can be found in the National CUI Registry.

        i. When used, CUI Category or Subcategory Markings are separated from the CUI Control Marking by a double forward slash (//).

        ii. When including multiple categories or subcategories in a portion, CUI Category or Subcategory Markings are separated from each other by a single forward slash (/)

When CUI Portion Markings are used and a portion does not contain CUI, a “U” is placed in parentheses to indicate that the portion contains Uncontrolled Unclassified Information.



D. CUI On Spreadsheets & Forms: Forms that contain CUI must be marked accordingly when filled in. If space on the form is limited, cover sheets can be used for this purpose.
As forms are updated during Department-wide implementation of the CUI Program, they should be modified to include a statement that indicates the form is CUI when filled in.

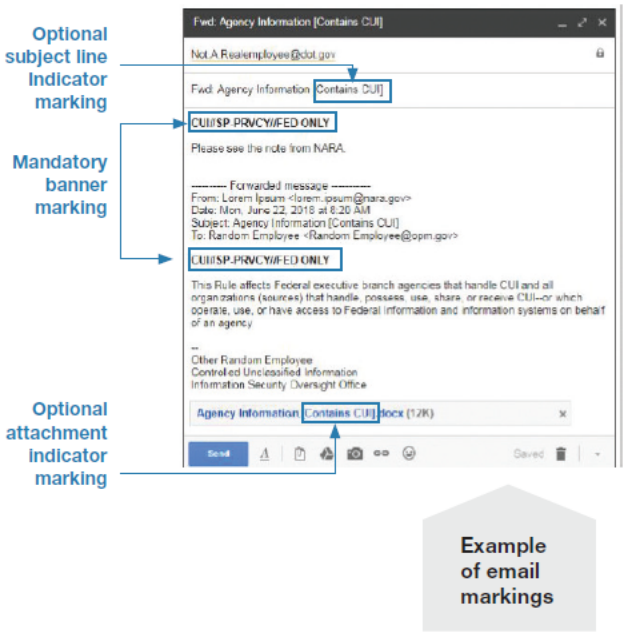
E. Marking Emails: It is mandatory to include CUI Banner Markings to indicate that an email contains CUI.

1. If an email is forwarded, the banner marking must be carried forward.

2. If sending an attachment that contains CUI, the name of the file can contain a CUI indicator.

3. If an attachment is removed, and the email no longer contains CUI, add the following statement below the banner marking "**Uncontrolled Unclassified Information**."

4. Emails that contain CUI must be encrypted.



APPENDIX C: CNSI MARKING GUIDE

Standard markings must be applied to all classified information. Except in extraordinary circumstances, or as approved by the Director of ISOO, the marking of classified information created after September 22, 2003, shall not deviate from the following prescribed formats.

If markings cannot be affixed to specific classified information or materials, the originator shall provide holders or recipients of the information with written instructions for protecting the information. Marking shall be uniformly and conspicuously applied to leave no doubt about the classified status of the information, the level of protection required, and the duration of classification.

A. Original Classification

On the face of each originally classified document, regardless of the media, the OCA shall apply the following markings.

1. Classification authority: The name or personal identifier, and position title of the OCA shall appear on the ``Classified By'' line. An example might appear as:

   Classified By: David Smith, Chief, Division 5, Department of Good Works, Office of Administration

   or

   Classified By: IDIMNO1, Chief, Division 5, Department of Good Works, Office of Administration

2. Agency and office of origin: If not otherwise evident, the agency and office of origin shall be identified and follow the name on the ``Classified By'' line. An example might appear as:

   Classified By: David Smith, Chief, Division 5 Department of Good Works, Office of Administration.

3. Reason for classification: The OCA shall identify the reason(s) for the decision to classify. The OCA shall include, at a minimum, a brief reference to the pertinent classification category(ies), or the number 1.4 plus the letter(s) that corresponds to that classification category in section 1.4 of EO 13526.

   a. These categories, as they appear in EO 13526, are as follows:

i. Military plans, weapons systems, or operations;

ii. Foreign government information;

iii. Intelligence activities (including special activities), intelligence sources or methods, or cryptology;

iv. Foreign relations or foreign activities of the United States, including CONFIDENTIAL sources;

v. Scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism;

vi. U.S. Government programs for safeguarding nuclear materials or facilities;

vii. Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to national security, which includes defense against transnational terrorism; or

viii. Weapons of mass destruction.

b. An example might appear as:

Classified By: David Smith, Chief, Division 5, Department of Good Works, Office of Administration

Reason: Vulnerabilities or capabilities of plans relating to the national security

or

i. When the reason for classification is not apparent from the content of the information, e.g., classification by compilation, the OCA shall provide a more detailed explanation of the reason for classification.

4. Declassification instructions: The duration of the original classification decision shall be placed on the ``Declassify On'' line. The OCA will apply one of the following instructions:

a. The OCA will apply a date or event for declassification that corresponds to the lapse of the information's national security sensitivity, and that is less than 10 years from the date of the original decision. When linking the duration of classification to a specific date

or event, mark that date or event as:

Classified By: David Smith, Chief, Division 5, Department of Good Works, Office of Administration

Reason: 1.4(g)

Declassify On: October 14, 2004,

or

Declassify On: Completion of Operation

b. When a specific date or event within 10 years cannot be established, the OCA will apply the date that is 10 years from the date of the original decision. For example, on a document that contains information classified on October 14, 2003, mark the ``Declassify On'' line as:

Classified By: David Smith, Chief, Division 5, Department of Good Works, Office of Administration

Reason: 1.4(g)

Declassify On: October 14, 2013

c. Upon the determination that the information must remain classified beyond 10 years, the OCA will apply a date not to exceed 25 years from the date of the original decision. For example, on a document that contains information classified on October 10, 2003, mark the ``Declassify On'' line as:

Classified By: David Smith, Chief, Division 5, Department of Good Works, Office of Administration

Reason: 1.4(g)

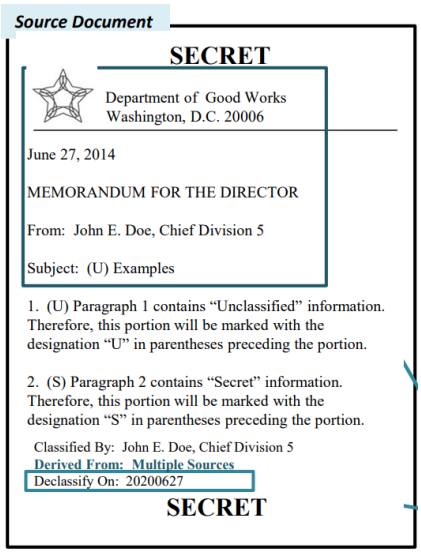
Declassify On: October 10, 2028

5. Overall marking: The highest level of classified information contained in a document shall appear in a way that will distinguish it clearly from the informational text.

a. Conspicuously place the overall classification at the top and bottom of the outside of the front cover (if any), on the title page (if any), on the first page, and on the outside of the back cover (if any).

b. For documents containing information classified at more than one level, the overall marking shall be the highest level. For example, if a document contains some information marked ``SECRET'' and other information marked ``CONFIDENTIAL,'' the overall marking would be ``SECRET.''

c. Each interior page of a classified document shall be marked at the top and bottom either with the highest level of classification of information contained on that page, including the designation ``Unclassified'' when it is applicable, or with the highest overall classification of the document.



6. Portion marking: Each portion of a document, ordinarily a paragraph, but including subjects, titles, graphics and the like, shall be marked to indicate its classification level by placing a parenthetical symbol immediately preceding or following the portion to which it applies.

a. To indicate the appropriate classification level, the symbols ``(TS)'' for TOP SECRET, ``(S)'' for SECRET, ``(C)'' for CONFIDENTIAL, and ``(U)'' for Unclassified shall be used.

b. Each classified portion of a document marked exempt from automatic declassification shall be exempted unless the OCA indicates otherwise on the document.

c. A waiver from the portion marking requirement for a specific category of information may be requested. Such a request shall be submitted to the Director of ISOO and should

include the reasons that the benefits of portion marking are outweighed by other factors. Statements citing administrative burden alone will ordinarily not be viewed as sufficient grounds to support a waiver.

7. Classification extensions: An OCA may extend the duration of classification for up to 25 years from the date of the information's origin for information contained in records determined to be permanently valuable.

    a. The ``Declassify On'' line shall be revised to include the new declassification instructions and shall include the identity of the person authorizing the extension and the date of the action.

    b. The office of origin shall make reasonable attempts to notify all holders of such information. Classification guides shall be updated to reflect such revisions.

    c. An example of an extended duration of classification may appear as follows for a document dated December 1, 2003, with a declassification date of December 1, 2015:

        Classified By: David Smith, Chief, Division 5, Department of Good Works, Office of Administration

        Reason: 1.4(g)

        Declassify On: Classification extended on December 1, 2005, until December 1, 2028, by David Jones, Chief, Division 5

8. Marking information exempted from automatic declassification at 25 years

    a. When an agency head or SAO exempts permanently valuable information from automatic declassification at 25 years, the ``Declassify On'' line shall be revised to include the symbol ``25X'' plus a brief reference to the pertinent exemption category(ies) or the number(s) that corresponds to that category(ies) in section 3.3(b) of EO 13526.. Other than when the exemption pertains to the identity of a CONFIDENTIAL human source, or a human intelligence source, the revised ``Declassify On'' line shall also include the new date or event for declassification. The marking for an exemption for the identity of a CONFIDENTIAL human source or a human intelligence source shall be ``25X1-human.'' This marking denotes that this specific information is not subject to automatic declassification.

    b. The pertinent exemptions, using the language of section 3.3(b) of EO 13526, are:

i. 25X1: reveal the identity of a CONFIDENTIAL human source, or a human intelligence source, or reveal information about the application of an intelligence source or method;

ii. 25X2: reveal information that would assist in the development or use of weapons of mass destruction;

iii. 25X3: reveal information that would impair U.S. cryptologic systems or activities;

iv. 25X4: reveal information that would impair the application of state-of-the-art technology within a U.S. weapon system;

v. 25X5: reveal actual U.S. military war plans that remain in effect;

vi. 25X6: reveal information, including foreign government information, that would seriously and demonstrably impair relations between the United States and a foreign government, or seriously and demonstrably undermine ongoing diplomatic activities of the United States;

vii. 25X7: reveal information that would clearly and demonstrably impair the current ability of United States Government officials to protect the President, Vice President, and other individuals for whom protection services, in the interest of the national security, are authorized;

viii. 25X8: reveal information that would seriously and demonstrably impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, infrastructures, or projects relating to the national security; or

ix. 25X9: violate a statute, treaty, or international agreement.

c. The pertinent portion of the marking would appear as:

Declassify On: 25X-State-of-the-art technology within a U.S. weapon system, October 1, 2020

or

Declassify On: 25X4, October 1, 2020

d. Documents should not be marked with a ``25X'' marking until HUD has been informed that the President or the Interagency Security Classification Appeals Panel concurs with the proposed exemption. Agencies that have submitted proposed exemptions or a declassification guide to the ISCAP may mark documents with ``25X'' categories, while waiting for ISCAP concurrence, unless otherwise notified by the Panel's Executive Secretary.

e. ``25X'' marking shall not be applied to individual documents contained in a file series exempted from automatic declassification under section 3.3(c) of the Order until the individual document is removed from the file.

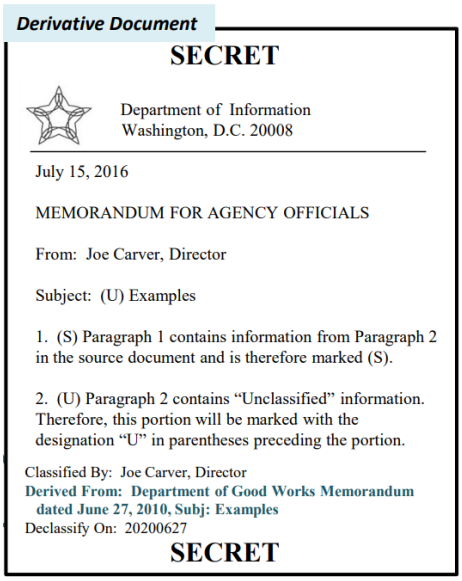
B. Derivative Classification Marking

1. All applicable classification markings, declassification instructions, handling instructions, and the identity of the derivative classifier, by name, position or personal identifier, shall be placed on the newly created material.

2. The derivative classifier must conspicuously mark the classified document with the highest level of classification of information included in the document.

3. Conspicuously place the overall classification at the top and bottom of the outside of the front cover (if any), on the title page (if any), on the first page, and on the outside of the back cover (if any).

4. For documents containing information classified at more than one level, the overall marking must be the highest level. For example, if a document contains some information marked “SECRET” and other information marked “CONFIDENTIAL,” the overall marking would be “SECRET.”



5. Each interior page of a classified document must be marked at the top and bottom either with the highest level of classification of information contained on that page, including the designation "unclassified" when it is applicable, or with the highest overall classification of the document.

6. Portion Marking: Each portion of a derivatively classified document, ordinarily a paragraph, but including subjects, titles, graphics, and the like, must be marked to indicate its classification level by placing a parenthetical symbol immediately preceding the portion to which it applies.

    a. To indicate the appropriate classification level, the symbols "(TS)" for TOP SECRET, "(S)" for SECRET, "(C)" for CONFIDENTIAL, and (U) for Unclassified must be used.

    b. Each classified portion of a document marked exempt from automatic declassification must be exempted unless the OCA indicates otherwise on the document.

7. Questions on classification markings, as the markings appear on the source or in a security classification guide, shall be referred to the originator. For challenges to classification refer to Chapter 3: Classification Challenges, of this Handbook.

8. If practical, where classified information constitutes a small portion of an otherwise unclassified document, the Derivative Classifier shall use a classified addendum and/or prepare a product in unclassified form to allow for maximum dissemination.