HOWARD UNIVERSITY POLICY
CONTROLLED UNCLASSIFIED INFORMATION

Policy Number:	Series: Academics and Research
Policy Title:	100-021: RESEARCH SECURITY AND CONTROLLED UNCLASSIFIED INFORMATION (CUI) POLICY
Responsible Officers:	Provost and Chief Academic Officer delegated to Associate Vice President and Institutional Official, Regulatory Research Compliance
Responsible Offices:	Office of Regulatory Research Compliance (ORRC) Office of Research Office of Audit and Compliance (OAC) Enterprise Technology Services (ETS)
Effective Date:	July 1, 2025

I. INTRODUCTION

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

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

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

NARA established a CUI Registry on its website as the authoritative reference for all CUI categories and markings.

II. RATIONALE

This Policy and Procedure implements EO 13556 and 32 CFR Part 2002, entitled *Controlled Unclassified Information*. These directives institute a national policy on the handling, safeguarding, and control of information the government creates or possesses

that a law, regulation, or government-wide policy requires or specifically permits an institution such as Howard University (HU) and Affiliated/Component Institutions to handle using approved safeguarding or dissemination controls. Classified information is not part of the CUI Program.

All unclassified information used and cultivated throughout the research process that requires any safeguarding or dissemination control is CUI**.** No safeguarding or dissemination controls for unclassified information may be implemented unless they are consistent with the CUI Program.

III. AUTHORITY

This Policy, Research Security and *Controlled Unclassified Information (CUI) Policy (*hereafter, the "Research Security Policy"), is issued under the authority and directive of the Howard University Office of Regulatory Research Compliance (ORRC) in the Office of the Provost, and in collaboration with the Office of the General Counsel**.**

IV. ENTITIES AFFECTED BY THIS POLICY

This Research Security Policy, predicated on the FOA/Designating Agency regulations, sets forth policy for the handling, marking, protecting, destroying, and decontrolling of CUI for the HU engagements, subject to CUI FOA/Designating Agency regulations. This Policy applies to all faculty, staff, students, and contractor employees who may encounter CUI in the performance of official duties at Howard University and Affiliates.

The provisions of this Policy shall not be construed to interfere with or impede the authorities or independence of HU Offices with the official responsibility to oversee Compliance Programs, including Research Security and CUI.

V. LIMITATIONS ON THE APPLICABILITY OF THIS POLICY [§ 2002.22]

Any CUI requirements contained within this Research Security Policy that are not supported by law, regulation, or government-wide policy may not be applied. When entering into agreements, HU may not include additional requirements or restrictions on handling CUI other than those permitted in federal laws and the CUI FOA/Designating Agency regulations.

VI. DEFINITION [§ 2002.4].

A. Agreements and Arrangements are any vehicle that sets up specific CUI handling requirements for contractors and other information-sharing partners when the arrangement with the other part involves CUI.

a. 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.

b. HU employees or contractors and Component staff shall not disseminate or share CUI with anyone in a manner that contradicts federal laws and the FOA/Designating Agency regulations.

B. An authorized holder is an individual, FOA/Designating Agency, organization, or group of users permitted to designate or handle CUI, in accordance with this Policy and 32 CFR part 2002.

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

D. CUI is information the government creates or possesses, or that an entity creates or possesses for or on behalf of the government, that a law, regulation, or government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.

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

F. CUI Basic is the subset of CUI for which the authorizing law, regulation, or Government-wide policy does not set out specific handling or dissemination controls. HU and Affiliated Institutions will handle *CUI Basic* according to the uniform set of controls set forth in this part and the CUI Registry. *CUI Basic* differs from *CUI Specified*, and *CUI Basic* controls apply whenever *CUI Specified* ones do not cover the involved CUI.

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

H. CUI Registry is the online repository for all information, guidance, policy, and requirements on handling CUI, including everything issued by the CUI EA. Among other information, the CUI Registry identifies all approved CUI categories, provides general descriptions for each, identifies the basis for controls, establishes markings, and includes guidance on handling procedures.

I. **Decontrolling** occurs when an authorized holder, consistent with this Policy and the CUI Registry, removes safeguarding or dissemination controls from CUI that no longer require such controls. Federal Oversight (FOA)/Designating Agency may decontrol automatically or through agency action. See §2002.18.

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

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

L. **The Office of the General Counsel** is responsible for the legal sufficiency review of all changes to the Research Security Policy.

M. **Handling** is any use of CUI, including but not limited to marking, safeguarding, transporting, disseminating, reusing, and disposing of the information.

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

O. **Legacy Material** is unclassified information that the FOA/Designating Agency and compliant HU and Affiliated CUI programs have marked as restricted from access or dissemination in some way or otherwise controlled before the CUI Program.

P. **Legacy Marking** is the marking / labeling originally used for such Legacy Material.

Q. **Legacy Information** is information that was never marked as CUI and does not contain a Legacy Marking but should be evaluated to determine whether it could reasonably be considered to contain CUI presently.

R. **Limited Dissemination Controls** is any CUI EA-approved control that the FOA/Designating Agency may use to limit or specify CUI dissemination.

S. **Misuse of CUI** occurs when someone uses CUI in a manner not in accordance with the FOA/Designating Agency and Howard University's Research Security Policy, the CUI Registry, 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 FOA/designating or marking information as CUI when it does not qualify as CUI.

T. IO -- Institutional Official-Compliance: The University Designated Institutional Official (IO) in the Office of Regulatory Research Compliance (ORRC) shall fulfill this responsibility. Thus, the HU IO is responsible for ensuring that HU has sufficient policies and guidance (based on EA guidance) for its faculty, staff, students, and contractors handling CUI. The IO will liaise with the FOA/Designating Agency and ensure compliance with applicable Federal regulations.

U. CUI-SAO – The Howard University Senior Administrative Official (Cabinet Member).

V. CUI-PM -- Controlled Unclassified Information Program Manager: The HU CUI-PM is responsible for managing the day-to-day programmatic HU CUI and the affiliate's activities, developing and implementing SOP premised on the HU's CUI Policy, complying with HU CUI Policy, ensuring that the HU CUI program and Components comply with federal and the HU Export Control and the National Institute of Standards and Technology (NIST 800-171) policies where applicable. Also, the CUI-PM will monitor compliance and other responsibilities as mandated by law and the HU CUI program**.** The CUI-PM prepares the annual CUI report, liaises with the CUI-SAO and CUI-IO, and submits it to the FOA/Designating Agency.

W. CUI-CPO -- Controlled Unclassified Information – Chief Privacy Officer (CPO). The HU leadership designates the CUI-CPO and has HU-wide responsibility for privacy, including implementation of privacy protections; compliance with Federal privacy laws, regulations, and policies; management of privacy risks at HU; and a central policy-making role.

X. FOUO means "For Official Use Only."

Y. SBU means "Sensitive But Unclassified."

Z. POC means Designated CUI "Points of Contact" within each CUI enclave. This person is likely the CUI Lead Investigator or CUI component manager.

AA. LDCM means Limited Dissemination Control Markings

(Note: 32 CFR Part 2002.4 contains additional relevant definitions.)

VII. POLICY and IMPLEMENTATION

This CUI Policy shall protect all CUI in accordance with national directives, ensure that sharing partners exercise the same care, and remove any CUI controls on the information

once it is decontrolled. These policies include or identify all CUI that is routinely handled by HU and Affiliated Researchers.

Throughout implementation, Legacy Markings and safeguarding practices will exist simultaneously, but no Legacy Markings should be created and, as implementation progresses, they will eventually be phased out.

VIII. ROLES AND RESPONSIBILITIES

A. The Provost shall:

i. Ensure the University's support.
ii. Advocate for resources to implement, manage, and comply with the requirements of the National CUI Program.
iii. Guide and advocate for the approval of the CUI policies by the Policy Committee to implement the CUI Program.
iv. Ensure that all executive positions required for this Policy are filled.

B. The CUI-IO Representing the ORRC shall:

i. Develop and administer the HU CUI Policy.
ii. Ensure compliance with the applicable Federal regulations.
iii. Work with the CUI program leadership to establish processes and criteria for reporting and investigating misuse of CUI.
iv. Implement an education and training program pursuant to 32 CFR § 2002.30 to include monitoring for compliance with training requirements.
v. Ensure the training and education program for both basic and specified categories of CUI include sufficient information that allows all policy personnel to understand and carry out their obligations concerning protecting, storing, transmitting, transporting, and destroying CUI.
vi. Synergize collaboration among ETS, Facility Management, Campus Security, Housekeeping, the Chief Privacy Officer, the Office of the General Counsel, the HU Procurement Office, and the CUI leads in support of a compliant CUI program.
vii. Monitor compliance and report violations to the FOA as necessary.
viii. Designate additional ORRC personnel to specific CUI responsibilities as necessary.

C. CUI-Senior Administrative Official (SAO) (Senior Vice President for Research) shall:

i. Appoint the CUI Program Manager.
ii. Lead, direct, and oversee the HU's CUI Program.
iii. Ensure that HU develops and implements CUI Standard Operating Procedures (SOP).
iv. Ensure that the HU SOP is premised on the HU CUI Policy and use the SOP to manage the CUI program in compliance with EO 13556, 32 CFR Part 2002; NIST 800-171; and 48 CFR 252.204-7019 (1/05/2024) Notice of NIST SP 800–171 DoD Assessment Requirements.

v. Include all FOA/Designating Agency approved changes to the CUI in the annual report to the FOA /Designating Agency.
vi. Work with the ORRC, Office of Audits and Compliance, and HU Enterprise Technology Services (ETS) to develop and implement the HU's self-inspection program in compliance with NIST SP 800–171.
vii. Establish a process to accept and manage challenges to CUI status (including improper or absence of marking) in accordance with existing processes based on laws, regulations, and government-wide policies.
viii. Notify authorized recipients of any waivers (unless notice is otherwise prohibited by law or regulation).
ix. Submit to FOA/Designating Agency any law, regulation, or policy not already incorporated into the CUI Registry that HU proposes to use to inform the designation of unclassified information for safeguarding or dissemination controls for approval before use.
x. Reiterate a description of all FOA/Designating Agency existing waivers in the annual report to FOA/Designating Agency, along with the rationale for each waiver and, where applicable, the steps HU is taking to protect CUI.
xi. Submit requests for CUI decontrol by authorized holders to FOA/Designating Agency.
xii. Ensure that the CUI SOP includes a mechanism by which authorized holders at HU and Affiliated Institutions can request instructions if and when they receive unmarked or improperly marked information designated as CUI.

D. The CUI Program Manager shall:

i. Manage the day-to-day operations of HU's CUI Program as mandated by the Policy and directed by the CUI-SAO.
ii. Develop an SOP congruent with the Research Security Policy and coordinate its implementation and updates.
iii. Manage the CUI Program, including liaising with Components POC on operations and related matters and submitting required reports.
iv. Liaise with the ORRC on the HU CUI compliance with the applicable Federal Regulations, government-wide requirements, and HU SOP.
v. Work with the ORRC/CUI-IO or designees as necessary to investigate and lead mitigation efforts for incidents involving CUI and report same to the CUI-IO and FOA/Designating Agency.
vi. Inform the CUI-IO and FOA/Designating Agency of any significant CUI incidents and any incident trends found within the HU and Component Institutions.
vii. Ensure compliance with the ORRC training recommendations and documents and communicate reports to the CUI-IO.
viii. Liaise with the ORRC while consolidating status reports from the components and forwarding HU reports to FOA.
ix. Maintain an internal website available for all employees to use that contains information about the CUI Program, with a section for each component to list their frequently encountered CUI categories and special instructions.

x. Update and maintain the University's Security Manual to include CUI protocols, including Marking, Handling, Dissemination, Access and Transmission Storage requirements, Decontrolling and Destruction, and Incident reporting.

E. The Chief Information Officer (Chief Security Officer) shall safeguard CUI in HU's Systems by:

i. Assessing all HU's systems that contain CUI.
ii. Ensuring that all information technology systems used to process CUIs meet the federal baseline of moderate confidentiality.
iii. Incorporating appropriate security measures into enterprise IT systems that contain CUI.
iv. Coordinating with the FOA/Designating Agency on system security to comply with CUI requirements.
v. Ensuring that information systems that process, store, or transmit CUI comply with Federal Information Processing Standards (FIPS) PUB 199 and 200, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 and 800-53, and other federal IT requirements.
vi. Developing, deploying, and guiding acceptable methods of protecting CUI within IT systems and transmitting CUI from HU's email systems.
vii. Developing, deploying, and guiding acceptable methods of protecting CUI on public-facing websites and in cloud-based systems.
viii. Ensuring information systems that contain CUI have the appropriate CUI Markings as per NIST SP 800-171, the NARA CUI Marking Handbook, and applicable agency guidance.
ix. Restricting the printing of CUI-related documents and the use of stick discs on CUI computers.
x. Developing robust guidelines for travel laptops.
xi. Working with the CUI-PM to:

1. Ensure that equipment is in place that meets CUI requirements for destroying CUI when HU no longer needs the information and HU's records disposition schedule no longer requires retention of the records in accordance with NIST SP 800-171; SP 800-52 and SP 800-88.
2. Destroy CUI, including CUI in electronic form, in a manner that makes it unreadable, indecipherable, and irrecoverable in accordance with NIST SP 800-88, Guidelines for Media Sanitization.
3. Ensure that physical facilities that contain CUI have appropriate CUI markings as per 32 CFR 2002.

F. Designated CUI Points of Contact (POC) and Alternates shall:

i. Complete all required CUI training congruent with the Research Security Policy and SOP.
ii. Conduct oversight actions to ensure compliance within their area of responsibility and report findings at least annually to HU's CUI-PM.
iii. Respond to most inquiries from the organizations and consult with the CUI-PM on questions beyond their expertise.

iv. Ensure all personnel within their component complete initial and recurring training as required and report the progress of training to the HU-PM and IO.
v. Conduct annual self-inspections of the CUI Program to reflect implementation progress and report the results of those self-inspections to the CUI-PM and IO.
vi. Report instances of potential CUI violations or infractions to the CUI-PM and IO and keep track of violations for reporting purposes.
vii. Confirm status as the CUI-POC with the CUI-PM and the CUI-SAO on a semi-annual basis (by the dates designated by the CUI-PM and FOA/Designating Agency) and provide notification within five business days if their status changes.

G. Contracting Officers and Contracting Officer Representatives (CORs):

i. The Associate/Assistant Vice President of Procurement and Contracts shall have oversight of this responsibility.
ii. Include the applicable federal and HU CUI security clauses in their assigned contracts.
iii. Ensure contractors are aware of and understand the CUI security clauses in their contracts.
iv. Include in all contracts, which may involve CUI, a clause requiring that the contractor comply with NIST SP 800-171 for any non-federal computer system they operate that contains CUI (see 32 CFR 2002.14(h)(2) for more information)
v. Include the appropriate requirements of this Policy in all procurement actions that relate to CUI.
vi. Ensure contractors receive training on CUI within 60 days of employment and before accessing CUI.

H. The HU Chief Privacy Officer (CUI-CPO) shall:

i. Coordinate with the CUI-PM and CUI-IO on all policies and procedures relating to the Privacy Act and Personally Identifiable Information (PII) to ensure consistency with the CUI framework and requirements.
ii. Ensure HU's compliance with privacy laws, regulations, and privacy policies applicable to CUI and this policy.
iii. Conduct audits of the CUI program as required in accordance with NIST SP 800-171 (48 CFR 252.204-7019 (1/05/2024) Notice of NIST SP 800–171 DoD Assessment Requirements.

I. Supervisors and Managers shall:

i. Review and ensure that all CUI products are properly marked in accordance with this policy, as needed.
ii. Verify that all physical safeguarding measures for individual workspaces are adequate for the protection of CUI (i.e., prevent unauthorized access) annually.
iii. Verify that all electronic safeguarding measures are adequate for the protection of CUI (i.e., prevent unauthorized access) annually.

iv. Ensure that all personnel under their purview receive CUI training as required by this policy (i.e., initial, recurring, and CUI Specified)
v. Comply with all CUI Policies and SOPs.

J. Employees, Contractor Employees, Interns, and Others as Designated Persons shall:

i. Complete all initial, recurring, and *CUI Specified* assigned CUI training within the required timeframes.
ii. Manage, mark, and protect CUI in accordance with this Policy and national directives.
iii. Ensure that sensitive information currently stored as legacy material that is annotated as For Official Use Only (FOUO), or Sensitive But Unclassified (SBU), or that contains other legacy security markings is re-marked as CUI before the information leaves HU.
iv. Ensure that only markings that are contained in the NARA CUI Registry may be used to annotate CUI.
v. Report incidents as needed.

IX. SAFEGUARDING [§ 2002.14]

A. The objective of safeguarding is to prevent the unauthorized disclosure of, or access to, CUI.

B. Unless different protection is specified in the CUI Registry, CUI (including CUI in burn bags) must be stored in a locked office, drawer, or locked file cabinet whenever 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.

C. Individuals working with *CUI Specified* must comply with the safeguarding standards outlined in the underlying law, regulation, or government-wide policy in addition to those described in this Policy.

D. Safeguarding During Working Hours:

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

E. Other Precautions:

i. Personnel should reasonably ensure that unauthorized individuals cannot access or observe CUI or overhear conversations where CUI is discussed.

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

iii. When outside a controlled environment, personnel must always keep the CUI under their direct control or protect it with at least one physical barrier and reasonably ensure that they or the physical barrier protects the CUI from unauthorized access or observation.

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

F. Care While Traveling:

i. CUI shall not be viewed while on public transportation where others may be exposed to it. CUI should be kept in a locked briefcase or room safe when in hotel rooms. 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.

ii. HU, Affiliated/Components CUI programs may not require more restrictive safeguarding standards than those described in this Policy or 32 CFR Part 2002 for their contractors or other authorized partners with whom they share CUI.

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

A. IT systems containing CUI must, at a minimum, meet NIST's Moderate Confidentiality standard. [See HU Enterprise Technology Services (ETS) Data Safety/NIST SP 800-171 compliant policy].

B. In accordance with FIPS PUB 199, CUI Basic is categorized at no less than the moderate confidentiality impact level. FIPS PUB 199 defines security impact levels for federal information and federal information systems. The appropriate security requirements and controls identified in FIPS PUB 200 and NIST SP 800-53 must be applied to CUI in accordance with any risk-based tailoring decisions made. With the agreement of FOA/Designating Agency, HU may increase CUI Basic's confidentiality impact level above moderate only within HU/Affiliated CUI programs, including contractors operating an information system on behalf of HU. HU 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 HU. The FOA should be consulted as needed.

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

iii. A federal information system is an information system used or operated by a federal agency or a contractor of an agency or other organization on behalf of an agency. Information systems that HU or affiliates operate on behalf of an agency are subject to the requirements of the CUI Program as though they are the agency systems, and the applicable agency may require these systems to meet the same requirements as its own internal systems.

iv. A non-federal information system is any information system that does not meet the criteria for a federal information system. Personnel may not treat non-federal information systems as though they are government systems. Therefore, employing non-federal information systems, HU follows the requirements of NIST SP 800-171 to protect CUI Basic unless specific requirements are specified by law, regulation, or government-wide policy for protecting the information's confidentiality.

D. NIST Special Publication 800-171 contains standards that HU and HU affiliates, component institutions, and contractors must meet if they have agency CUI on their computer systems.

E. Systems authorized to store, process, and/or transmit classified information are considered sufficient for the protection of CUI, provided that access, dissemination, and marking protections are adhered to.

XI. DESTRUCTION [§ 2002.14(f)]

A. CUI may be destroyed:

i. When the information is no longer needed, and

ii. When records disposition schedules, published or approved by NARA or other applicable laws, regulations, or government-wide policies, no longer require retention.

B. Destruction of CUI, including in electronic form, must be accomplished in a manner that makes it unreadable, indecipherable, and irrecoverable. CUI may not be placed in office trash bins or recycling containers. CUI Specified must be destroyed according to any specific directives regarding the information. If the authority does not specify a destruction method, HU-approved personnel must use one of the following methods:

i. 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: Controlled Unclassified Information (CUI) and Multi-Step Destruction Process.

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

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

A. Predicated upon LDCM guidance on the National Archive's CUI Registry website, HU may disseminate and permit access to CUI, provided that such access or dissemination:

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

ii. Furthers a lawful HU CUI or Government purpose.

iii. Is not restricted by an authorized LDCM established by the CUI EA.

iv. Is not otherwise prohibited by law.

v. Is in concordance with the CUI FOA/Designating Agency.

B. Only the Limited Dissemination Controls Markings (LDCM) published in the CUI Registry may be used to restrict the dissemination of CUI to certain individuals, agencies, or organizations. These dissemination controls may only be used to further a lawful HU CUI or government purpose if laws, regulations, or government-wide policies require or permit their use. Personnel should consult with and follow the FOA/Designating Agency(s) regulation if there is significant doubt about using an LDCM.

ii. If significant doubt remains after consulting the Policy, please consult with the CUI-IO and the FOA/Designating Agency(s) for further guidance.

iii. LCDM includes government-approved CUI HU employees and affiliates, principal investigators, federal employees, and contractors only. No foreign dissemination or dissemination to contractors. Dissemination list controlled is (dissemination authorized only to those individuals, organizations, or entities included on an accompanying dissemination list) authorized for release to certain nationals only and display only. **See the National Archive's CUI Registry for LDCM guidelines: https://www.archives.gov/cui/registry/limited-dissemination.**

C. HU CUI may not impose controls that unlawfully or improperly restrict access to CUI.

D. In addition to the requirements listed above, should there be a need for CUI to be shared with any non-HU personnel or entity, it shall be done only with documented

approval of the FOA/Designating Agency and CUI-SAO under the following conditions:

i. When there is a reasonable expectation that all intended recipients have a lawful purpose for receipt of CUI, are authorized to receive the CUI, and have a basic understanding of how to handle it.
ii. Whenever feasible, components shall enter into some type of formal information-sharing agreement with the recipient of the CUI. The agreement must include a requirement for the recipient to, at a minimum, comply with EO 13556, 32 CFR Part 2002, and the CUI Registry.
iii. Foreign entity sharing [2002.16(a)(5)(iii)]. When entering into information-sharing agreements or arrangements with a foreign entity, personnel should encourage that entity to protect CUI in accordance with EO 13556; 32 CFR Part 2002; and the CUI Registry. The personnel with access to CUI are cautioned to use judgment as to what and how much to communicate, keeping in mind the ultimate goal of safeguarding CUI. Only the CUI markings and controls may be allowed if such agreements or arrangements include safeguarding or dissemination controls on unclassified information. Other markings or protective measures may not be used.
iv. Information-sharing agreements made before the establishment of the CUI Program should be modified whenever feasible, so they do not conflict with CUI Program requirements. [§ 2002.16(a)(5)(iv)]
v. 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-IO. CUI-IO must report any non-compliance to the FOA/designating agency. [§ 2002.16(a)(6)]

E. CUI Basic may be disseminated to persons and entities meeting the access requirements of this section. HU may further restrict the dissemination of CUI Basic by using an authorized LDCM published on the CUI Registry.

F. Authorized recipients of CUI Basic may further disseminate the information to individuals or entities meeting and complying with the requirements of this CUI Program and LDCM. CUI Specified may only be disseminated to persons and entities as authorized in the underlying legislation, policy, or authority contained in the CUI Registry. Further dissemination of CUI Specified may be made to authorized persons if not restricted by the underlying authority (governing law, regulation, or HU policy). As in the case of CUI Basic, CUI Specified may further restrict the dissemination of CUI Specified using authorized LDCMs. https://www.archives.gov/cui/registry/limited-dissemination.

XIII. DECONTROL OF CUI [§ 2002.18]

A. When control is no longer needed, HU SAO, in collaboration with CUI-IO and with the concordance of the FOA/Designating Agency, should decontrol any CUI it designates. This means the information should be removed from the protection of the CUI program as soon as practicable when the information no longer requires safeguarding or dissemination controls unless doing so conflicts with the underlying authority.

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

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

ii. When the FOA/Designating Agency decides to release the CUI to the public by making an affirmative, proactive disclosure.

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

1. Disclosures under FOIA constitute CUI decontrol for all purposes.
2. 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).

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

C. FOA/Designating Agency may also decontrol CUI:

i. In response to a request from an authorized holder to decontrol it.

ii. 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.

D. A CUI component may designate in its CUI SOP which personnel it authorizes to decontrol CUI, consistent with law, regulation, and FOA/Designating Agency policy.

E. 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.

F. When CUI has been decontrolled by the FOA/Designating Agency, personnel must clearly indicate that CUI is no longer controlled when restating, paraphrasing, re-using, or releasing to the public. Otherwise, personnel do not have to mark, review, or take other actions to indicate the CUI is no longer controlled.

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

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

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

I. If an authorized holder publicly releases CUI in accordance with the FOA/Designating Agency's authorized procedures, upon consultation with the FOA/Designating Agency, the release constitutes decontrol of the information.

J. Unauthorized disclosure of CUI does not constitute decontrol.

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

L. When laws, regulations, or FOA/Designating Agency policies require specific decontrol procedures, personnel must follow such requirements.

Records Management Note: *The Archivist of the United States may decontrol records transferred to the National Archives in accordance with 32 CFR Part 2002.34, absent a specific agreement to the contrary with the FOA/designating agency. The Archivist decontrols records to facilitate public access pursuant to 44 U.S.C. 2108 and NARA's regulations at 36 CFR parts 1235, 1250, and 1256. When decontrol is not feasible prior to transfer, the CUI status of the information is indicated on a Transfer Request or an SF 258 paper form. Any other indication of CUI status, such as markings on the container, are not valid.*

XIV. MARKING OF CUI [§ 2002.20]

A. CUI markings listed in the CUI Registry are the only markings authorized to designate unclassified information requiring safeguarding or dissemination controls.

B. Personnel and authorized holders must, in accordance with the implementation timelines established by the FOA/Designating Agency and within HU's CUI policies and procedures:

   i. Discontinue all use of legacy or other markings not permitted or included in the CUI Registry.
   ii. Uniformly and conspicuously apply CUI markings to all CUI exclusively in accordance with the CUI Registry, unless the FOA/Designating Agency has issued a limited CUI marking waiver.

C. Information may not be marked as CUI:

   i. To conceal violations of law, inefficiency, or administrative error
   ii. To prevent embarrassment to the U.S. Government, any U.S. official, organization, or agency.
   iii. To improperly or unlawfully interfere with competition.
   iv. To prevent or delay the release of information that does not require such protection.
   v. If the CUI is required by law or regulation to be made available to the public or if it has been released to the public under proper authority.

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 the policy and the CUI Registry.

E. When it is impractical for a component to individually mark CUI due to the quantity or nature of the information, or when the FOA/Designating Agency 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 using user access agreements, computer system digital splash screens, or signs in storage areas or containers.

F. 32 CFR Part 2002, the CUI Registry, NIST 800-171, and NARA's supplemental guidance (CUI Marking Handbook) shall be followed for marking CUI on paper and electronic documents. The handbook was developed to assist authorized holders by providing examples of correctly marked CUI.

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

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

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

iii. Limited Dissemination Control Markings. NARA has published a list of several Limited Dissemination Control Markings that can be applied based on FOA/Designating Agency's criteria. These markings will appear in the CUI Registry and will include such controls as FED ONLY (Federal Employees Only), NOCON (No dissemination to contractors), and DL ONLY (Dissemination authorized only to those individuals or entities on an accompanying distribution list). Limited Dissemination Control Markings are preceded by a double forward slash (//) and appear as the last element of the CUI banner marking.

1. Limited Dissemination Control Markings may only be applied to CUI to bring attention to any dissemination control called for in the underlying authority or to limit the dissemination of CUI. Limited Dissemination Control Markings should be used only after carefully considering the potential impacts on the timely dissemination of the information to authorized recipients.

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

I. Specific marking, disseminating, informing, distribution limitation, or warning statements that are required by underlying authorities may also be placed on the document but not within the banner or portion markings. These markings or indicators must be placed on the document as prescribed by the underlying law, regulation, or government-wide policy. Questions regarding the placement of such markings may be referred to the responsible authority for the information.

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

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

Incorrectly marked documents. If personnel believe that CUI is marked incorrectly, they should provide notice of the error to their respective CUI POC within their organization and the disseminating entity or the FOA/Designating Agency.

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

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

B. Portion marking is not required, but it is permitted and encouraged to facilitate information sharing and proper handling and to assist FOIA reviewers in identifying the CUI within a large document that may be primarily Uncontrolled Unclassified Information

C. If portion markings are used in any portion of a document, they must be used throughout the entire document. All portions or sections must be portion marked, even those that do not contain CUI. Sections that do not contain CUI should be marked as Uncontrolled Unclassified Information, designated with a [U].

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

A. When authorized holders include CUI in documents containing CNSI, the CUI Program's decontrolling provisions apply only to portions marked as CUI. In addition, personnel must:

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

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

B. The CUI Registry and the NARA CUI Marking Handbook contain specific guidance on marking CUI when commingled with CNSI. https://www.archives.gov/files/cui/documents/20161206-cui-marking-handbook-v1-1-20190524.pdf https://www.archives.gov/cui/registry/limited-dissemination?_ga=2.48227623.1446504821.1731433635-437078721.1731433635

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

A. In-transit tracking, though optional, is recommended for CUI unless otherwise stated by the FOA/Designating Agency. CUI may be sent through the United States Postal Service or any commercial delivery service that offers in-transit automated tracking and accountability tools.

B. CUI may also be sent through authorized interoffice mail systems.

C. Address packages and parcels containing CUI for delivery only to a specific recipient, NOT 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.

D. Double wrapping CUI when it is being transported is optional unless otherwise stated by the FOA/Designating Agency.

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

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

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

   i. "When the enclosure is removed, this document is Uncontrolled Unclassified Information."

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

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

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

B. When reproducing CUI documents on equipment such as printers, copiers, scanners, or fax machines, management officials must ensure that the equipment does not retain data or transmit the data to a non-federal entity, or else they must sanitize it in accordance with NIST SP 800-53. Before purchasing equipment, management should ensure that it does not store or transmit data to non-federal entities and that at the end of the equipment's lifecycle, any hard drives or memory is sanitized per NIST SP 800-88.

XX. WORKING PAPERS [§ 2002.20(k)]

A. Working papers (drafts) are documents or materials, regardless of form, that HU personnel, affiliates, or users expect to revise before creating a finished product.

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

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

A. Supplemental administrative markings (e.g., "Pre-decisional," "Deliberative," "Draft") may be used with CUI. The NARA CUI Marking Handbook provides examples of supplemental administrative markings. https://www.archives.gov/cui/registry/category-marking-list

B. Supplemental administrative markings may not impose additional safeguarding requirements or disseminating restrictions or designate the information as CUI. Their purpose is to inform recipients of the status of documents under development to avoid confusion and maintain the integrity of a decision-making process.

C. Supplemental markings, other than the universally accepted "DRAFT," shall, on the first page or the first time it appears, include an explanation or intent of the marking, e.g.,

   i. Pre-decisional – "The information in this document provides background, options, and/or recommendations about [topic]. It is not yet an accepted policy." (This is an example only. The language may be changed to suit the topic.)

D. Supplemental markings may not appear in the CUI banners nor be incorporated into the CUI designating/decontrolling indicators or portion markings.

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

XXII. UNMARKED CUI [§ 2002.20(m)]

A. Unmarked information that qualifies as CUI should be marked and treated appropriately as described in this policy.

XXIII. CUI SELF-INSPECTION PROGRAM [§ 2002.24]

A. In accordance with 32 CFR § 2002.8(b)(4), HU CUI and its affiliates will implement a Self-Inspection Program as follows:

i. The CUI PM and HU CIO, under the authority of the CUI-IO, shall provide technical guidance, training, and materials for HU components to conduct reviews and assessments of their CUI Programs at least annually and to report the results to the FOA/Designating Agency as required.

ii. Following the training of the designated CUI POCs, components shall conduct annual self-inspections of their CUI Programs and report the results on a schedule determined by the CUI-IO. Components 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.

iii. Predicated on the SOP and following guidance and inspection materials developed by the CUI PM, self-inspection methods, reviews, and assessments shall serve to evaluate program effectiveness, measure the level of compliance, and monitor the progress of CUI implementation.

iv. Based on the SOP developed by the CUI-PM and guided by the CUI Policy, the CUI PM shall provide to the components formats for documenting self-inspections and recording findings and provide advice for resolving deficiencies and taking corrective actions.

v. Results from the HU-wide and components self-inspections shall inform updates to the CUI training provided to the components.

.

XXIV. EDUCATION AND TRAINING [§ 2002.30]

A. Every HU employee, official, detailee, intern, and contractor employee who may encounter CUI in their work shall complete initial CUI awareness training immediately upon hiring, before engaging any CUI-related responsibilities and not to exceed 60 days after employment. Refresher training shall be required every two years after the initial training. Personnel must also take training for any CUI-specified categories they have access to or for which they are required to safeguard.

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

XXV. CUI COVER SHEETS [§O 2002.32]

A. Personnel may use cover sheets to identify CUI, alert observers that CUI is present from a distance, and to serve as a shield to protect the attached CUI from inadvertent disclosure.

B. Though optional, the HU CUI-PM shall obtain and use Cover Sheets - Form (OF) 901, OF 902, and OF 903 as the only authorized CUI cover sheets. Cover Sheets may be obtained from the Office of Security Programs and may then be reproduced by the HU CUI-PM office. OF 901 may also be ordered from GSA. OF 902 and OF 903 contain space to add categories or warning notices and may be downloaded from the NARA site as follows:

i. Standard Form 901 (SF 901): General CUI markings

https://www.gsa.gov/system/files/SF901-18a.pdf

ii. SF 902: Identify media such as hard drives that contain CUI

https://www.archives.gov/cui/additional-tools

iii. SF 903: Identify media devices such as USB drives that contain CUI

https://www.archives.gov/cui/additional-tools

*(**NOTE**: SF-901 replaces the following: OF 901, OF 902, OF 903)*

XXVI. LEGACY MATERIALS [§ 2002.36]

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

B. Documents created before November 14, 2016 (and before HU CUI implementation) must be reviewed and re-marked if they contain information that qualifies as CUI. If HU and FOA/Designating Agency do not re-mark the Legacy Material as CUI, an alternate permitted marking method must be used.

C. The following protocols shall guide components in the proper handling of Legacy Material when it is encountered during the implementation of the CUI Program:

i. Receiving Legacy Material when the recipient has implemented the CUI Program:

1. If the receiving HU personnel or affiliate has not been certified to receive CUI, such persons should not receive Legacy Material.

2. If the receiving HU personnel or affiliate plans to reuse or transmit the Legacy Marked information, then it must evaluate the information and remark it as CUI in consultation with the FOA/Designating Agency.
3. If applicable, receiving HU personnel or affiliate handling CUI must also adhere to FOA/Designating Agency marking waivers as they apply to internal dissemination.
4. If applicable, all receiving HU personnel or affiliates handling CUI will apply any appropriate Limited Dissemination Control Markings (LDCMs).

ii. Receiving HU personnel or affiliates should NOT reuse legacy markings, such as FOUO or SBU, on new documents that are derived from Legacy Material.

1. HU personnel or affiliates should contact the originator of the material if they have any questions.

iii. Receiving information marked as CUI when the recipient has NOT implemented the CUI Program:

1. Transmitting HU personnel or affiliates may feel some trepidation about the security of their information when the recipient has not implemented the CUI Program, as the recipient may not inherently protect this information to the same standards outlined in the CUI Program. For this reason, the transmitting HU personnel or affiliates may wish to convey safeguarding requirements for this information to the receiver directly.
2. Recipients must then protect this information in accordance with any safeguarding guidelines from the originators of the material, individual agency policy, and/or any LDCM.
3. Recipients shall complete initial CUI awareness training before engaging any CUI-related responsibilities. Refresher training shall be required every two years after the initial training. Also, recipients must take training for any CUI-specified categories they will have access to or for which they are required to safeguard.

iv. Receiving HU personnel or affiliates should NOT remove CUI markings from the information.

v. HU personnel or affiliates should contact the originator of the material or the FOA/Designating Agency if they have any questions.

vi. Sending information marked as CUI when the recipient has NOT implemented the CUI Program:

1. The transmitting HU personnel or affiliates must keep their CUI markings on the information.

2. In compliance with the Information System Security Officer (ISOO) recommendations, if CUI Specified or LDCM are contained in the transmission of the information, the sender should also include a description of the safeguarding or dissemination requirements related to the information.
3. Transmitting HU personnel or affiliates should use the SF Form 901 to express these additional safeguards to recipients.

vii. Sending Legacy Marked information when the recipient has implemented the CUI Program:

1. Transmitting HU personnel or affiliates must provide a point of contact with the information in case the recipient has questions about safeguarding the material.
2. Any special handling requirements associated with the information, such as limited dissemination controls, should be conveyed through transmittal or in a manner apparent to the recipient of the information.

XXVII. WAIVERS OF CUI REQUIREMENTS [§ 2002.38c]

A. The CUI FOA/Designating Agency may approve waivers of all or some of the CUI marking requirements while the CUI remains within HU if it is determined that, due to a substantial amount of stored information with legacy markings, removing legacy markings or re-marking it as CUI would be excessively burdensome.

B. When an authorized holder re-uses any Legacy Material or information derived from Legacy Material or Legacy Information that qualify as CUI, they must remove or redact legacy markings and designate or re-mark the information as CUI, even if the information is under a legacy material marking waiver prior to re-use.

C. In exigent circumstances, when a waiver is required, the HU CUI program, in collaboration with the CUI-IO, will consult with the FOA/Designating Agency to consider waiving certain requirements of the CUI Program for any CUI while it is within HU and its affiliates' possession or control unless specifically prohibited by applicable laws, regulations, or HU policies.

D. Exigent circumstances waivers may apply when HU is requested to share the information with other Federal Agencies. HU employees shall NOT share CUI with non-authorized or non-federal entities unless directed by the appropriate FOA/Designating Agency (s) through established secured communication to the SAO. In such cases, recipients must be made aware of the CUI status of any disseminated information.

E. Waivers approved by the authorized FOA/Designating Agency are valid only while the information remains within HU. CUI markings must be uniformly and conspicuously applied to all CUI prior to disseminating it outside HU unless otherwise specifically permitted by NARA.

F. Per 32 CFR Part 2002.38(e), the CUI-SAO and CUI-PM shall:

i. Retain a record of each waiver.
ii. Include a description of all current waivers and waivers issued during the preceding year in the annual report to FOA/Designating Agency, along with the rationale for each waiver and the alternate steps the agency takes to ensure sufficient protection of CUI.
iii. Follow the instruction of the FOA/Designating Agency on notifying authorized recipients and the public of these waivers through means such as notices or websites.
iv. Inform the CUI-IO as permitted by law.

XXVIII. CUI AND DISCLOSURE STATUTES [§ 2002.44]

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

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

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

XXIX. CUI AND THE PRIVACY ACT [§ 2002.46]

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

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

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

   i. The System Security Plan and the FIPS 199 confidentiality, integrity, and availability risk level determinations for the system.

   ii. Any Paperwork Reduction Act compliance documentation completed prior to collection of information from the public.

   iii. The applicable Privacy and Civil Liberties Impact Assessment, which discusses:

      1. The applicable Privacy Act SORN for the records maintained in the information system (which should also be consulted).
      2. Any applicable information-sharing agreements.
      3. Handling requirements mandated by law with respect to particular information in the system.
      4. With whom the information is shared internally and externally.

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

A. Authorized holders of CUI who, in good faith, believe that a designation as CUI is improper or incorrect or who believe they have received unmarked CUI should notify the HU CUI-PM of this belief. Challenges may be made anonymously, and challengers cannot be subject to retribution for bringing such challenges. The

CUI-PM shall promptly report the incident to the CUI-IO, OGC, and FOA/Designating Agency.

B. If the information at issue is involved in litigation, or the challenge to its designation or marking as CUI arises as part of litigation, whether the challenger may access the information will be addressed via the litigation process instead of by the CUI-PM. Challengers should notify the CUI-PM of the issue through the process described below, including its litigation connection.

C. If the HU Office receives a challenge, the HU CUI-POC shall work with the HU CUI-PM to take the following measures:

   i. Acknowledge receipt of the challenge

   ii. Provide an expected timetable for response to the challenger.

   iii. Review the merits of the challenge internally with CUI-IO, OGC, as well as the FOA/Designating Agency Subject Matter Expert.

   iv. Offer an opportunity to the challenger to define a rationale for the belief that the CUI in question is inappropriately designated.

   v. Notify the challenger of the HU decision.

   vi. Provide contact information of the official making the decision in this matter.

   vii. Inform the CUI-SAO, CUI-IO, and the CIO and CPO (as appropriate), and the FOA/Designating Agency.

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

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

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

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

B. Suspected or confirmed CUI misuse shall be reported immediately to the HU's CUI-PM. The CUI-PM shall obtain the details of the situation, coordinate with a FOA/Designating Agency Subject Matter Expert regarding the severity of the incident, and share the results of the investigation with the CUI-SAO and CUI-IO within 48 hours of discovery. The CUI POC (Lead Investigator) should coordinate mitigation measures as appropriate within their management structure and provide regular status reports to the CUI-PM until mitigation efforts are complete.

C. Reportable CUI incidents include, but are not limited to:

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

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

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

iv. 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.

v. 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.

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

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

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

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

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

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

D. The CUI-PM, in conjunction with the CUI-IO, shall determine if sanctions to the offender are appropriate or if other corrective action may be warranted (e.g., emphasis on training). Misuse of CUI shall be reported to the FOA/Designating Agency(s).

XXXII. SANCTIONS FOR MISUSE OF CUI [§ 2002.56]

A. Misuse of CUI can result in disciplinary action, up to and including removal from HU or recommendation for removal to the POC at the Component Institution. In the event an HU contractor employee misuses CUI, the matter shall be referred to the cognizant contracting officer to determine whether remedies should be imposed under the contract.

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

   i. Severity of the incident.
   ii. Intent of the person committing the incident.
   iii. Extent of training the person(s) has received.
   iv. Frequency of which the individual has been found responsible in the commission of other such incidents, including Security Violations or Infractions involving classified information.

C. Sanctions include but are not limited to verbal or written counseling, reprimand, suspension from duty and pay, removal, removal of access to CUI, suspension or revocation of access to classified information, termination of classification authority, or criminal penalties. The underlying law, regulation, or HU policy/Component Institution (as relevant) is consulted for guidance, as appropriate.

D. Administrative sanctions are assessed per the policies, procedures, and practices established by the HU/Component Institution's Human Resources Office, and actions involving the suspension or revocation of a security clearance are taken per the applicable Executive Orders and ODNI policies and regulations.

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

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

XXXIII. PUBLICATION OF CUI

A. Publication of CUI or its posting on public websites or social media is prohibited unless the CUI has been properly decontrolled in accordance with section XIII above.

B. CUI-PM, CUI-POCs/Components, front-line supervisors, and the ORRC should routinely review HU and Component websites and social media sites to ensure that CUI is not posted.

XXXIV. REQUESTING NEW CATEGORIES OF CUI

A. Personnel who encounter information described in law, regulations, or HU policy that is not described in the CUI Registry may recommend that a new information category be entered into the Registry.

B. Personnel should submit their recommendation directly to the HU's CUI-PM or through Component POC to the HU CUI-PM. For components, including affiliates, the CUI Component POC shall coordinate through their legal counsel's office and submit a recommendation to the CUI-PM. The request should include:

i. A description of the information to be marked as CUI.

ii. The law(s), regulation(s), or the HU CUI Policy.

iii. The name of the category applicable to the information.

iv. A suggested name, along with a suggested acronym for the category.

REFERENCES[1]

EO 13556, Controlled Unclassified Information, November 4, 2010

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

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

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

NIST Special Publication (SP) 800-53, Revision 5 Security and Privacy Controls for Federal Information Systems and Organizations, as updated through November 2023

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

NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, Revision 1, December 2016, as corrected by Revision 2, January 28, 2021.

National Archives and Records Administration (NARA) NARA CUI Marking Handbook: https://www.archives.gov/files/cui/documents/20161206-cui-marking-handbook-v1-1-20190524.pdf

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

48 CFR 252.204-7019 (up to date as of 1/05/2024). Notice of NIST SP 800–171 DoD Assessment Requirements.

CUI Registry: Limited Dissemination Controls
https://www.archives.gov/cui/registry/limited-dissemination?_ga=2.48227623.1446504821.1731433635-437078721.1731433635

CROSS-REFERENCES

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

For Optimal Compliance With The Applicable Federal Regulation, The Howard University Policy Builds Upon/Uses The US Department of Energy Policy Template:
https://www.directives.doe.gov/ipt_members_area/idoe-o-471.x-ipt/doe-documents/generalized-cui-policy-template/view