IT/IM DIRECTIVE POLICY

Directive No: CIO 2158.2

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

Controlled Unclassified Information (CUI) Policy

1. PURPOSE

This policy establishes the U.S Environmental Protection Agency's (EPA) requirements for safeguarding and dissemination controls of Controlled Unclassified Information (CUI) and sets forth the framework to implement Executive Order (E.O.) 13556 and 32 Code of Federal Regulations (CFR) § 2002, both titled, "Controlled Unclassified Information." This policy is the foundational document from which all procedures, standards, and guidelines, and other EPA directives will be developed in defining and implementing CUI requirements for the agency. CUI must be protected from unauthorized access during collection, use, dissemination, and storage. This policy provides authorization for the National CUI Program that establishes the processes EPA shall use to govern the program, informs agency employees and managers about their roles and responsibilities, and details the consequences for non-compliance with requirements of the CUI policy.

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

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

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

On September 14, 2016, NARA issued a final rule amending 32 CFR § 2002 to establish a uniform policy for all federal agencies on designating, safeguarding, disseminating,

marking, decontrolling, and disposing of CUI; self-inspection and oversight requirements; and other facets of the program.

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

2. SCOPE

This policy applies to:

- All CUI, regardless of format, that EPA creates, possesses, receives, or that an entity creates or possesses for or on behalf of EPA, that is required or specifically permitted to be protected under law, regulation, or government-wide policy. All unclassified information throughout EPA and the Executive Branch that requires CUI safeguarding or dissemination control(s) pursuant to a law, regulation, or government-wide policy is considered CUI**.** The official list of all CUI categories is found in the U.S. National Archives and Records Administration's (NARA) CUI Registry. Only CUI categories listed on the CUI Registry are authorized for protection of CUI and must be handled consistently with the National CUI Program as defined in this policy and any subsequent procedures, standards, and guidelines. CUI shall serve as the exclusive designation for identifying sensitive but unclassified information throughout the Executive Branch of Government to include EPA. Classified information is not part of this program as it falls under E.O. 13526, Classified National Security Information as of December 29, 2009, or the Atomic Energy Act.

- Anyone who handles CUI, including those who handle CUI under arrangements, agreements, contracts, and other transaction authority actions, requiring access to CUI according to terms and conditions including, but not limited to, grants, licenses, certificates, memoranda of agreement/arrangement or understanding, and information-sharing agreements or arrangements (see 32 CFR § 2002.4(c)).

3. AUDIENCE

This policy applies to all EPA employees, contractors, grantees, and all other users of EPA information and information systems supporting the operations and assets of EPA. EPA's CUI policy does not apply to entities outside the agency unless a law, regulation, or government-wide policy requires or permits the controls contained in the agency policy to do so, and the CUI Registry lists that law, regulation, or government-wide policy as an authority (32 CFR § 2002.22). EPA's CUI policy does not apply directly to

non-executive branch entities but does apply indirectly to non-executive branch recipients of CUI, through incorporation into agreements (32 CFR § 2002.1(f)).

4. AUTHORITY

This CUI Policy Directive is issued under the authority of EPA's Chief Information Officer (CIO), pursuant to delegation 1-19, dated 07/07/2005. Any disciplinary action shall be guided by E.O. 9830, as amended, and chapters 43 and 75 of Title 5, U.S. Code.

Legal foundations for the policy include:

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

5. POLICY

It is EPA policy to protect CUI by using proper safeguarding and dissemination controls in accordance with 32 CFR § 2002. This policy sets forth the overarching directive for the designating, marking, handling, decontrolling, and destroying of CUI for EPA. This policy and related information directives establish EPA's CUI Program and requirements for implementing CUI practices in a phased approach.

- Implementation. EPA has begun implementing CUI practices (designating, marking, safeguarding, disseminating, destroying, and decontrolling). EPA will phase out legacy markings and safeguarding practices as implementation proceeds.

- Program Offices and Regions. All Program Offices and Regions are required to implement CUI practices according to EPA CUI policy and to protect all CUI in accordance with applicable procedures, standards, and guidelines. Additionally, Regions and Program Offices must ensure that information-sharing partners exercise the same care and remove any CUI controls on the information once it is decontrolled.

- Agreements. Written agreements (e.g., Memoranda of Understanding (MOUs), Interagency Agreements (IAs), other agreement vehicles) involving CUI shall adhere to this policy. Written agreements and safeguarding controls must be in place prior to the sharing of CUI.

- Contracts. Contracting Officers (CO) and Contracting Officer Representatives (COR) must include the requirement for compliance with 32 CFR § 2002 and Federal Acquisition Regulations (FAR) in any contracts involving CUI.

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

- Marking and Safeguarding. All CUI documents must be protected according to applicable laws, regulations, and government-wide policies. Specific procedures for marking and labeling are outlined in the subsequent CUI procedures, standards, and guidelines. Information systems processing, storing, or transmitting CUI must meet the security and privacy protections at the moderate confidentiality baseline, as defined in FIPS PUB 199, FIPS PUB 200, and NIST Special Publication 800-53r5. Anyone who has access to CUI will be held accountable for knowing and following these procedures as described in this policy and subsequent CUI procedures, standards, and guidelines.

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

Information should not be designated CUI in order to:

- Conceal violations of law, inefficiency, or administrative error;
- Prevent embarrassment to a person, organization, or agency;
- Prevent open competition;
- Control information not requiring protection under a law, regulation, or government-wide policy.

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

Designation as CUI does not determine whether that information should be released under the Freedom of Information Act (FOIA), and the applicability of FOIA exemptions does not determine whether information should be designated as CUI. Employees should follow EPA's existing FOIA policy and procedures to determine if information is exempted from release. Any perceived conflicts should be addressed by the EPA CUI Program Manager (PM), who must receive concurrence from the respective FOIA program within EPA for resolution.

6. ROLES AND RESPONSIBILITIES

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

EPA Chief Information Officer (CIO):

a) Ensures senior leadership support and adequate resources are available for implementation, management, and oversight of the CUI Program.
b) Issues and promulgates CUI policy, procedures, standards, and guidelines to ensure that EPA complies with all CUI requirements in accordance with 32 CFR § 2002.
c) Ensures EPA's strategic plans include CUI compliance requirements.
d) Ensures enforcement and compliance with CUI and related information directives.
e) Ensures that CUI management processes are integrated with agency strategic and operational planning processes.
f) Designates the EPA Senior Agency Official for Controlled Unclassified Information (SAO for CUI) in writing. EPA SAO for CUI must be at the Senior Executive Service (SES) level or equivalent.
g) Oversees the activities of the EPA SAO for CUI.

h) Reviews and approves CUI annual reports to the CUI Executive Agent created by the CUI PM.

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

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

EPA CUI Program Manager (PM):

a) Designated by the EPA SAO for CUI.
b) Coordinates all aspects of the day-to-day activities of the EPA CUI Program, supported by CUI Liaisons from Program Offices and Regions with CUI responsibilities.
c) Chairs the EPA's CUI Advisory Committee (CUIAC) with CUI Liaison representatives from every Program Office and Region.
d) Develops agency-level CUI policy, procedures, standards, and guidelines.
e) Develops a CUI education and training program and ensures all agency personnel, including contractors and other affiliates, receive appropriate CUI Training.
f) Provides overall CUI management and policy guidance.
g) Develops and implements EPA's self-inspection program.
h) Establishes a process to accept and manage challenges to CUI statutes (e.g., improper or absence of marking), based on laws, regulations, and government-wide policies.
i) Submits official CUI annual reports to the CUI Executive Agent on behalf of the SAO for CUI.
j) Represents EPA at government-wide NARA meetings (e.g., CUI Advisory Council, CUI Registry Committee).
k) Submits to the CUI Executive Agent any law, regulation, or government-wide policy not already incorporated in the CUI Registry that EPA proposes to use to designate unclassified information for safeguarding or dissemination controls.

l) Coordinates with the CUI Executive Agent, as appropriate, on any proposed law, regulation, or government-wide policy that would establish, eliminate, or modify a category of CUI, or change information controls applicable to CUI.
m) Coordinates with the CISO to ensure that Privacy and Security policy, procedures, standards, and guidelines are consistent with respect to safeguarding CUI.
n) Provides all existing waivers in the annual report to the CUI Executive Agent, along with the rationale for each waiver and, where applicable, the alternative steps EPA is taking to ensure sufficient protection of CUI within the agency.
o) Establishes processes for handling CUI decontrol requests.
p) Establishes processes and procedures for authorized holders (both inside and outside EPA) to be able to contact a designated agency representative for instructions upon receiving unmarked or improperly marked information that the agency has designated as CUI.
q) Communicates CUI Program updates to Program Offices and Regions, as needed.
r) Performs delegated responsibilities from the SAO for CUI as needed.

EPA Chief Information Security Officer (CISO):

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

Senior Information Officials (SIO):

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

CUI Liaisons:

a) Primary and alternate are designated by the SIO of their respective Regions or Program Offices.

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

EPA CUI Advisory Committee (CUIAC):

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

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

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

Supervisors and Managers:

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

All EPA employees, contractors, and other affiliates:

a) Mark, safeguard, and appropriately disseminate CUI when encountering and handling it.
b) Take the mandatory CUI training within 180 days of beginning employment and on an annual basis.

c) Immediately report any misuse of CUI, including unmarked or improperly marked CUI, in accordance with the agency's incident response procedures (EPA Directive CIO 2150-P-08.2, Information Security – Incident Response Procedures).

Agency Records Officers:

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

7. RELATED INFORMATION

- E.O. 13556 Overview for Departments and Agencies
- CUI Notices and Executive Agent Guidance
- EPA Controlled Unclassified Information (CUI) Procedure(s)
- Records Management Policy (CIO 2155.5)
- Information Security – Incident Response Procedures (CIO 2150-P-08.2)

The CIO Senior Advisory Council (SAC), OMS-EI, Program Offices, Regions, and laboratories will direct their workforce to comply with procedures and implementation guidelines for this policy as appropriate for the management of EPA's CUI Program.

8. DEFINITIONS

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

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

CUI is information the government creates or possesses, or that an entity creates or possesses for or on behalf of the government, that a law, regulation, or government-

wide policy requires or permits an agency to handle using safeguarding or dissemination controls. CUI does not include classified information or information a non-executive 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.

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

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

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

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

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

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

Legacy markings are markings applied prior to the start of the CUI Program on unclassified information that requires access or dissemination controls.

Misuse of CUI occurs when someone uses CUI in a manner not in accordance with the policy contained in E.O. 13556, 32 CFR § 2002, the CUI Registry, agency CUI policy, or the applicable laws, regulations, and government-wide policies that govern the affected information. This may include intentional violations or unintentional errors in safeguarding or disseminating CUI. This may also include designating or marking information as CUI when it does not qualify as such.

Non-executive branch entity is a person or organization established, operated, and controlled by individual(s) acting outside the scope of any official capacity as officers, employees, or agents of the executive branch of the Federal Government. Such entities may include: Elements of the legislative or judicial branches of the Federal Government; state, interstate, tribal, or local government elements; and private organizations. Non-executive branch entity does not include foreign entities as defined in 32 CFR § 2002, nor does it include individuals or organizations when they receive CUI pursuant to federal disclosure laws, including FOIA and the Privacy Act of 1974.

Additional definitions in 32 CFR § 2002.4 are incorporated by reference.

9. WAIVERS

The EPA SAO for CUI may approve waivers of all or some of the CUI marking requirements while the CUI remains within EPA, if it is determined that, due to a substantial amount of stored information with legacy markings, removing legacy markings or re-marking it as CUI would be excessively burdensome unless specifically prohibited by applicable laws, regulations, or government-wide policies. The application process for waivers is detailed in the subsequent CUI procedure.

10. DIRECTIVE(S) SUPERSEDED

Controlled Unclassified Information (CUI) Policy, CIO 2158.1, January 2023.

11. CONTACTS

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

VAUGHN NOGA Digitally signed by VAUGHN NOGA
Date: 2024.07.10 15:38:11 -04'00'

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