OPBM-NP-18-0001

UNITED STATES DEPARTMENT OF COMMERCE
Controlled Unclassified Information (CUI) Policy
August 2019

1. Purpose. To establish Department of Commerce (DOC) policy and framework in order to implement Executive Order 13556, Controlled Unclassified Information (CUI).

2. Background.

a. Executive Order (E.O.) 13556, Controlled Unclassified Information establishes an open and uniform program for managing unclassified information requiring safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies. Excluded is information that is classified under E.O. 13526, Classified National Security Information as of December 29, 2009, or the Atomic Energy Act, as amended.

b. In the past, agencies employed ad hoc, agency-specific policies, procedures, and markings to safeguard and control this information, and there was no Government-wide direction on what information should be protected. Under CUI program established by E.O. 13556 , the categories and subcategories 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.

c. On September 14, 2016 the National Archives and Records Administration (NARA) issued a final rule amending 32 CFR Part 2002 to establish a uniform

policy for agencies on designating, safeguarding, disseminating, marking, decontrolling, and disposing of CUI, self-inspection and oversight requirements, and other facets of the program.

d. The CUI Program covers any information that constitutes CUI as defined by, 32 CFR § 2002.4(h) and described in section 5 of this policy ("Definitions").

3. Roles.

a. CUI Executive Agent

(1) E.O. 13556 designates the NARA as the CUI Executive Agent to implement the CUI Program and oversee agency actions to ensure compliance with the E.O.

(2) The Information Security Oversight Office (ISOO), a NARA component, performs the duties assigned to NARA as the CUI Executive Agent.

(3) The CUI Advisory Council consists of representatives from each executive branch agency who work with the Executive Agent on CUI-related matters.

b. The DOC CUI Program Office

(1) DOC's Senior Agency Official (SAO) for CUI has overarching responsibility for the CUI Program within DOC. The Secretary has designated the DOC Chief Information Officer (CIO) as the SAO responsible for the DOC CUI program.

(2) DOC's CUI Program Manager is accountable to the SAO and is responsible for coordinating all aspects of the CUI Program, supported by personnel from other applicable DOC Offices with CUI responsibilities.

4. Applicability. This policy applies to:

a. All DOC personnel including, but not limited to, employees, contractor employees, and other associates;

b. As required by 32 CFR § 2002.4(c), as amended, all persons or entities that handle DOC CUI under agreements and arrangements that include CUI provisions, such as contracts, grants, licenses, certificates, memoranda of agreement/arrangement or understanding, and information-sharing agreements or arrangements.

c. Anyone responsible for DOC-controlled space, or for managing or procuring government-owned or leased space.

d. The Office of Inspector General (OIG) to the extent that the OIG determines this policy is consistent with the OIG's independent authority under the Inspector General Act of 1978, as amended, 5 U.S.C. App. and it does not conflict with other OIG policies or the OIG mission.

e. As limited by 32 CFR § 2002.22, DOC CUI policies do not apply to entities outside the agency unless a law, regulation, or Government-wide policy requires or permits the controls contained in the agency policy to do so, and the CUI Registry lists that law, regulation, or Government-wide policy as a CUI authority.

5. Definition. The DOC adopts the following definitions:

CUI – Information the government creates or possesses, or that an entity creates or possesses for or on behalf of the government, that a law, regulation, or government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. CUI does not include classified information or information a non-executive branch entity possesses or 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. Specific details about the types of information considered to be CUI can be found in NARA's final rule, 32 CFR Part 2002, as amended.

Misuse of CUI – When an individual uses CUI in a manner not in accordance with the policy contained in the DOC CUI policy and guidelines, E.O. 13556, 32 CFR Part 2002, the CUI Registry or the applicable law, regulation, or Government-wide policy that govern the affected information. This may include intentional violations or unintentional errors in safeguarding or disseminating CUI that results in unauthorized sharing of, or access to, that information in any form. This may also include designating or marking information as CUI when it does not qualify as CUI. Examples of reportable CUI incidents can be found in the DOC CUI Guidelines, Section 36.

Additional definitions are delineated in the CUI Guidelines, Section 8.

6. Policy. This policy and the DOC CUI Guidelines establish DOC's CUI Program and the DOC requirements for the handling, marking, disseminating, protecting, destroying, and decontrolling of CUI in accordance with 32 CFR Part 2002, as amended. The

Guidelines are incorporated herein in their entirety and carry the same force as this policy.

a. This policy is in agreement with the latest version of the DOC IT Security Policy and DOC Security Manual. Any perceived conflicts in these policies should be addressed to the CUI Program Manager for resolution.

b. This policy is not intended to supersede or conflict with requirements outlined in the Privacy Act of 1974, as Amended (5 U.S.C. 552a). When determining whether information must be protected under the Privacy Act or whether the Privacy Act allows for the release of information to an individual, the Department will base its decision on the content of the information and the Privacy Act's criteria, regardless of whether the information has been marked as CUI. Any perceived conflicts should be addressed to the CUI Program Manager, who must receive concurrence from the DOC Senior Agency Official for Privacy (SAOP), for resolution.

c. This policy is not intended to supersede or conflict with existing Departmental policy and practice in responding to requests for information under the Freedom of Information Act (FOIA). The marking of CUI does not exempt information from being considered responsive to a request under FOIA, nor is information deemed exempt from release under the FOIA inherently CUI. Any perceived conflicts should be addressed by the CUI Program Manager, who must receive concurrence from the DOC Chief FOIA Officer for resolution.

d. All DOC bureaus are required to implement CUI according to the DOC CUI policy and DOC CUI Guidelines.

7. Responsibilities. Below are the responsibilities of the CUI-specific roles established to implement the CUI program under E.O. 13556. Other roles and responsibilities for DOC offices and positions are detailed in the DOC CUI Guidelines.

a. Senior Agency Official (SAO) for CUI - The SAO must be at the Senior Executive Service level or equivalent. DOC's Senior Agency Official (SAO) for CUI is the Department Chief Information Officer. He/She is responsible for:

- Establishing and overseeing the CUI Program in DOC;

- Ensuring the agency has CUI implementing policies and plans;

- Implementing a CUI education and training program and ensuring agency personnel, including contractors as applicable, receive appropriate CUI awareness training;

- Providing updates on CUI implementation efforts to the CUI Executive Agent;

- Notifying authorized recipients, the Executive Agent, and the public of any waivers granted by DOC per procedures as written in CUI Guidelines, Section 31, Waivers of CUI Requirements. Annual reporting to the CUI Executive Agent must include a description of all waivers along with the rationale for each waiver and the alternative steps the agency is taking to ensure necessary protection of CUI within the agency;

- Developing and implementing the agency's self-inspection program;

- Establishing a process to accept and manage challenges to CUI status (including improper or absence of marking), in accordance with existing processes based in laws, regulations, DOC policy, and Government-wide policies;

- Establishing processes and criteria for reporting and investigating misuse of CUI;

- Monitoring and enforcing DOC's compliance with laws, regulations and government-wide OMB policy in collaboration with the DOC Chief Information Officer (CIO), SAOP, and Office of Security;

-Ensuring methods of destruction for print, electronic media and any other forms of CUI are established;

- Establishing processes for decontrolling CUI;

- Appointing and overseeing the activities and responsibilities of the DOC CUI Program Manager;

- In cases of CUI misuse, consult with relevant management as detailed in the Guidelines with respect to the applicability of sanctions;

- Submitting to the CUI Executive Agent any law, regulation, or Government-wide policy not already incorporated into the CUI Registry that the agency proposes to

use to designate unclassified information for safeguarding or dissemination controls; and

- Coordinating with the CUI Executive Agent, as appropriate, any proposed law, regulation, or Government-wide policy that would establish, eliminate, or modify a category or subcategory of CUI, or change information controls applicable to CUI.

b. CUI Program Manager (PM) - The CUI PM is appointed by the SAO for CUI and is responsible for:

- Managing the day-to-day operations of DOC's CUI program as directed by the SAO;

- Coordinating CUI policy development and updates;

- Organizing and overseeing CUI training efforts;

- Carrying out the responsibilities of the SAO that are delegated to the CUI Program Manager;

- Chairing a CUI Working Group to advise the SAO on the overall direction of the DOC CUI Program. The Working Group will meet regularly and follow the direction of the Working Group Charter. The Working Group [1]will consist of representatives from all Bureaus and Offices to recommend policies and procedures, research topics, coordinate plans, and provide recommendations to the SAO;

- Organizing and conducting DOC's CUI self-inspection program;

- In cases of CUI misuse and in consultation with the CUI SAO, making recommendations regarding sanctions, if any, to cognizant management; and

- Interacting directly and officially with the Executive Agent on CUI matters including submission of required reports.

c. Bureau Chief Information Officer (CIO)/Bureau CUI Point of Contact (POC). Most bureau CUI POCs are appointed from within the bureau's CIO organization as most CUI is commonly accessed through the electronic environment and CUI protective

[1] While the OIG will participate in this working group, it will not participate in the formulation of Department policy due to its oversight role and will function as an observing member of the group.

measures training is usually computer based. However, bureaus may appoint the Bureau CUI POC they deem most appropriate. They are responsible for:

- Establishing and overseeing the CUI Program in the bureau;

- Establishing bureau CUI implementing policies and plans;

- Providing representation to the DOC CUI Working Group to ensure bureau equities are considered;

- Ensuring bureau personnel, including contractors and/or associates as applicable, complete appropriate CUI awareness training;

- Providing updates on CUI implementation efforts to the DOC CUI PM;

- Ensuring bureau personnel adhere to DOC processes and criteria for reporting and investigating misuse of CUI;

- Ensuring bureau compliance with laws, regulations and Government-wide OMB policy reporting to DOC CUI PM;

- Assessing bureau systems that contain CUI and ensuring the systems that are used to process CUI meet the federal baseline of moderate confidentiality;

- Incorporating appropriate security and privacy measures into enterprise IT systems that contain CUI;

- Coordinating with the DOC CUI PM and DOC Chief Information Security Officer on IT system security to comply with CUI requirements;

- Ensuring that information systems that process, store, or transmit CUI are in compliance with Federal Information Processing Standard (FIPS) PUB 199 and 200, NIST Special Publication (SP) 800-53, and other federal IT requirements where applicable;

- Issuing guidance regarding acceptable methods of protecting CUI within IT systems and transmitting CUI from DOC email systems;

- Reporting misuse of CUI in accordance with the CUI Guidelines;

- Issuing guidance regarding acceptable methods of protecting CUI on public facing websites and in cloud-based systems; and

- Ensuring information systems that contain CUI have the appropriate CUI Markings as per 32 CFR Part 2002.

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

e. All DOC personnel, including but not limited to, employees, contractor employees, guest researchers, interns, and other associates or any authorized recipient of CUI are responsible for protecting and properly securing CUI materials and information as well as reporting its misuse in accordance with the DOC CUI Guidelines.

f. CUI Executive Agent (EA). The roles and responsibilities of the CUI EA are outlined in 32 CFR § 2002.8(a).

g. Additional specific responsibilities are defined in the DOC CUI Guidelines.

8. Training. Any individual as outlined in Section 7d who has access to CUI shall receive training annually. New employees and contractors must receive initial awareness training within 30 days of beginning employment and prior to access to CUI. The CUI Guidelines delineates the specifics of mandatory training.

9. 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 CUI Guidelines. Information systems processing, storing, or transmitting CUI must meet the security and privacy protections at the moderate confidentiality baseline as defined in NIST Special Publication 800-53. Anyone who has access to CUI will be held accountable for knowing and following these procedures as described in this policy and associated CUI Guidelines.

10. 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 Department Administrative Order (DAO) 202-751. Discipline and authorities listed

therein are set forth in E.O. 9830, as amended, and chapters 43 and 75 of Title 5, U.S. Code and the DOC CUI Guidelines, Section 36. Disciplinary actions relative to misuse of CUI are considered as "Violation of a security regulation" as listed in Appendix B, Table of Offenses and Penalties of DAO 202-751. In the event a contractor misuses CUI, the matter must be referred to the contracting officer to determine whether remedies should be imposed under the contract.

Misuse of CUI must be reported to the Bureau CUI POC and to the DOC CUI PM within 48 hours of discovery in accordance with the DOC CUI Guidelines, Section 35.

11. Contacts.

a. Contact with the Program Manager and/or SAO can be made via CUI@doc.gov.

b. Additional information about the CUI Program can be found at archives.gov/cui.

12. References.

a. Executive Order 13556 Controlled Unclassified Information (CUI)

b. 32 CFR Part 2002 Controlled Unclassified Information (CUI)

c. Department Organization Order 15-23, Chief Information Officer

d. Department Administrative Order 202-751, Discipline

e. Controlled Unclassified Information (CUI) Guidelines

f. NARA's CUI webpage

g. DOC CUI webpage

13. Signature.

Terryne F. Murphy [S] Aug 14 2019
Terryne F. Murphy
Senior Agency Official for CUI and Chief Information Officer (Acting)