GENERAL SERVICES ADMINISTRATION
Washington, DC 20405

CIO 2103.2
4/10/2021

GSA ORDER

SUBJECT: Controlled Unclassified Information (CUI) Policy

1. Purpose. To establish a General Services Administration (GSA) policy and framework for Controlled Unclassified Information (CUI). CUI is unclassified information that requires safeguarding and dissemination controls pursuant to law, regulation, or Government-wide policy, as listed in the CUI Registry by the National Archives and Records Administration (NARA).

2. Cancellation. This Order cancels and supersedes CIO 2103.1, Controlled Unclassified Information (CUI) Policy, dated May 16, 2017.

3. Revisions. The following updates have been made:

a. Updated links and terminology;

b. Added policy-related sections that were previously in the CUI Guide;

c. Added responsibilities previously in the CUI Guide; and

d. Added additional policies in the References section.

4. Background.

a. Executive Order (EO) 13556, Controlled Unclassified Information, establishes an open and uniform program for managing information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, or Government-wide policies, excluding information that is classified under Executive Order 13526 of December 29, 2009, or the Atomic Energy Act, as amended (hereinafter described as Controlled Unclassified Information (CUI)).

b. In the past, agencies employed ad hoc, agency-specific policies, procedures, and markings to safeguard and control sensitive information and there was no Government-wide direction on what information should or should not be protected. EO 13556

established a uniform program for managing CUI. Under the CUI Program, only the categories of information listed in the CUI Registry will be marked and handled as CUI.

c. On September 14, 2016, NARA issued a final rule amending 32 C.F.R. § 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 the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that is required to be protected under law, regulation, or Government-wide policy. This information 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 executive branch agency. Specific details about the types of information considered to be CUI are listed in the CUI Registry which can be found at archives.gov/cui.

5. Authorities.

a. CUI Executive Agent.

(1) Executive Order 13556 designates the National Archives and Records Administration (NARA) as the CUI Executive Agent (EA) to implement the CUI Program, oversee agency actions, and ensure compliance with the EO.

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

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

b. The GSA CUI Program Office.

(1) GSA's Senior Agency Official (SAO) for CUI has overarching responsibility for the CUI Program within GSA. SAO duties are assigned within GSA IT to the Deputy CIO in accordance with Chapter 9 of the GSA Delegations of Authority Manual, ADM 5450.39.

(2) GSA's CUI Program Manager (PM) is accountable to the SAO and is responsible for coordinating all aspects of the CUI Program, supported by Subject Matter Experts (SMEs) across the agency.

(3) All questions concerning CUI may be addressed to the SAO or CUI PM via cui@gsa.gov, or search the CUI FAQs or our webpage at InSite.gsa.gov/cui.

6. Applicability. This Order applies to:

a. All GSA employees;

b. All persons or entities that handle GSA CUI under agreements that include CUI provisions, to include contracts, grants, licenses, certificates, memoranda of agreement or understanding, and information-sharing agreements, as required by the amended 32 C.F.R. § 2002.4(c);

c. Anyone responsible for GSA-controlled space or for managing or procuring Government owned or leased space on behalf of GSA, as required in PBS 3490.3 CHGE 1 Security for Sensitive Building Information Related to Federal Buildings, Grounds, or Property;

d. The Office of Inspector General (OIG) to the extent that the OIG determines it is consistent with the OIG's independent authority under the IG Act, and it does not conflict with other OIG policies or the OIG mission; and

e. The Civilian Board of Contract Appeals (CBCA) to the extent that the CBCA determines it is consistent with the CBCA's independent authority under the Contract Disputes Act and other authorities and it does not conflict with the CBCA's policies or the CBCA mission.

7. Policy.

a. This Order implements the CUI Program at GSA and invokes the GSA CUI Guide which contains procedures and details for the handling, marking, protecting, sharing, destroying, and decontrolling of CUI in accordance with the amended 32 C.F.R. § 2002 and the CUI Registry.

b. This Order is consistent with CIO 2100.1 GSA Information Technology (IT) Security Policy and CIO 2200.1 GSA Privacy Act Program. Any perceived conflicts with these policies should be addressed to the CUI PM who will coordinate with the appropriate leadership to resolve any conflict.

c. PBS 3490.3 CHGE 1 Security for Sensitive Building Information Related to Federal Buildings, Grounds, or Property is a specific policy pertaining to the handling of Public Buildings Service (PBS) building information that is sensitive. PBS 3490.3 CHGE 1 will remain separate due to its unique nature, but falls within the GSA CUI Program.

8. Responsibilities. The responsibilities described below are assigned to the organizations and positions identified to ensure effective implementation and management of the CUI Program.

a. GSA Administrator. In accordance with 32 C.F.R. § Part 2002, agency heads are responsible for:

(1) Ensuring senior leadership support;

(2) Making adequate resources available to implement, manage and comply with the requirement of the CUI Program;

(3) Designating the CUI Senior Agency Official responsible for oversight of the CUI Program;

(4) Approving agency policies, as required, to implement the CUI Program; and

(5) Ensure establishment of a self-inspection program to ensure the agency complies with the principles and requirements of 32 C.F.R. § 2002 and the CUI Registry.

b. Senior Agency Official (SAO) for CUI.

(1) Direct and oversee the CUI Program within GSA, and request adequate resources to implement, manage, and comply with the CUI Program;

(2) Appoint and oversee the activities and responsibilities of the GSA CUI PM;

(3) Ensure the agency has CUI implementing policies and plans;

(4) Implement and maintain a CUI education and training program and ensure agency personnel including contractors, if applicable, receive appropriate CUI awareness training;

(5) Provide reports and updates on CUI implementation efforts to the CUI EA;

(6) Submit to the CUI EA 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;

(7) Coordinate with the CUI EA 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;

(8) Establish processes for handling CUI decontrol requests submitted by authorized holders;

(9) Notify authorized recipients, the CUI EA, and the public of any waivers granted by GSA, including a description of all waivers in the annual report to the CUI EA, along with the rationale for each waiver and, where applicable, the alternative steps GSA is taking to ensure sufficient protection of CUI within the agency;

(10) Develop and implement GSA’s self-inspection program;

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

(12) Establish a process to accept and manage challenges to CUI status in accordance with existing processes based in laws, regulations, or Government-wide policies;

(13) Establish processes and criteria for reporting and investigating misuse or improper handling of CUI;

(14) Assist with and respond to audits conducted by the CUI EA;

(15) Ensure GSA's compliance with laws, regulations, and policies in collaboration with the GSA CIO, the Senior Agency Official for Privacy (SAOP) and the Office of General Counsel;

c. CUI Program Manager (PM).

(1) Manage the day-to-day operations of GSA's CUI Program as directed by the SAO;

(2) Coordinate CUI policy development and updates;

(3) Carry out the responsibilities of the SAO that are delegated to the CUI PM;

(4) Interact directly and officially with the CUI EA on CUI matters including submission of required annual reports and any other reports that may be requested;

(5) Serve as the official representative on the CUI Advisory Council that is managed by the CUI EA;

(6) Serve as GSA's SME in CUI, advising the agency on the CUI Program and ensuring operations comply with Government-wide requirements;

(7) Coordinate efforts to investigate and lead mitigation efforts, for incidents involving CUI, and informing the CUI SAO of any significant CUI incidents as well as any trends found within GSA;

(8) Organize and oversee CUI training efforts;

(9) Implement the agency's CUI self-inspection program;

(10) Coordinate with GSA representatives from applicable Service and Staff Offices (SSOs) in order to guide program implementation and management of the program; and

(11) Maintain a CUI webpage on InSite for employees and contractors to refer to for information about the CUI Program.

d. Heads of Service and Staff Offices (HSSOs).

(1) Ensure systems and applications are compliant with GSA's CUI Policy and Guide. Any costs associated with needed upgrades/changes should be budgeted and planned for in order to meet the date set for full operational capability of the CUI Program;

(2) Make adequate resources available to implement, manage, and comply with the CUI Program;

(3) Ensure that their organizations actively implement the CUI Policy, CUI Guide, other procedures, and hold accountable all personnel within their respective organization;

(4) Ensure that authorized users who handle CUI, comply with the safeguarding requirements of the CUI Guide;

(5) Ensure that authorized users complete GSA's mandatory CUI Training within 60 days of joining GSA and at least every 2 years thereafter; and

(6) Ensure any applicable policies and procedures are consistent with the CUI Policy and Guide.

e. Chief Information Officer (CIO).

(1) Ensure that IT systems that process, store, or transmit CUI are in compliance with Federal Information Processing Standards (FIPS) publications (PUB) 199 and 200, National Institute of Standards and Technology (NIST) special publication (SP) 800-53, Federal Information Security Modernization Act (FISMA), 32 C.F.R. § 2002, and other federal IT requirements with regards to CUI;

(2) Issue guidance regarding acceptable methods of protecting CUI within IT systems, on public facing websites, and in cloud-based and email systems; and

(3) Ensure proper management of the CUI Program.

f. Senior Agency Official for Privacy (SAOP). Has agency-wide responsibility and accountability for the GSA Privacy Program, in accordance with OMB Memorandum M-16-24, and therefore will ensure GSA's compliance with privacy laws, regulations, and GSA privacy policies applicable to CUI.

g. Enterprise Data and Privacy Management Office (IDE).

(1) Serve as the SME for privacy-related issues, and provide ongoing support with matters concerning the Privacy Program and its connection with the CUI Program;

(2) Provide oversight of the CUI Program in coordination with the CUI SAO and the CUI PM;

(3) Coordinate with the CUI PM on all policies and procedures relating to treating CUI as records; and

(4) Ensure proper records disposition schedules are in place for when retention of records containing CUI is no longer required.

h. Office of Chief Information Security Officer (OCISO).

(1) Assess GSA's IT systems that contain CUI and ensure that all IT systems, applications, and projects that are used to process CUI meet the required moderate confidentiality impact level;

(2) Incorporate appropriate security measures into enterprise IT systems that contain CUI;

(3) Coordinate with the CUI team on IT system's security to ensure compliance with CUI requirements; and

(4) Coordinate with the CUI team when CUI-related incidents are reported.

i. Office of Digital Infrastructure Technologies (IDT). Coordinate with GSA Incident Response Team and the CUI PM regarding IDT's Knowledge Base articles and processes for the GSA IT Service Desk personnel and their handling of CUI-related incidents.

j. Office of Mission Assurance (OMA). Assist the CUI SAO with the physical and personnel security aspects of the CUI Program.

k. Office of Administrative Services (OAS).

(1) Ensure that equipment or processes are in place that meet CUI requirements for destroying CUI; and

(2) Provide additional support related to CUI needs with regards to training, safeguarding, destroying, marking, and sharing CUI, and any other applicable requirements.

l. Authorizing Officials (AOs), Program Managers, System Owners, Information Security System Managers (ISSMs), and Information System Security Officers (ISSOs).

(1) Determine the IT systems that contain CUI;

(2) Implement and manage the CUI Program requirements as applicable for each system; and

(3) Maintain systems to be compliant with GSA's CUI Guide and 32 C.F.R. § 2002.

m. GSA Contracting Officers (COs) and Contracting Officer Representatives (CORs).

(1) Ensure that the appropriate requirements of GSA's CUI Guide and NIST SP 800-171 are included in all procurement actions that relate to CUI as specified in the Federal Acquisition Regulation (FAR) and General Services Acquisition Manual; FAR Case 2017-016 "Controlled Unclassified Information" has been opened for reference;

(2) Comply with CUI requirements associated with sensitive procurement documents; and

(3) Ensure applicable contractors are aware of and understand the requirements of CUI clauses in their contracts, including any training requirements.

n. Supervisors and Managers.

(1) As applicable, review and ensure, as applicable, that all CUI is properly marked in accordance with GSA's CUI Guide and GSA's CUI Marking Manual;

(2) Comply with GSA's CUI Self-Inspection Program and ensure employees, and applicable contractors, comply;

(3) Verify regularly that all physical safeguarding measures for workspaces and office areas are adequate for the protection of CUI as needed;

(4) Verify regularly that all electronic safeguarding measures are adequate for the protection of CUI; and

(5) Ensure that all personnel under their purview receive CUI training as required by CUI policies.

o. All Employees, Contractors, and any Others Subject to GSA's CUI Policy.

(1) Everyone working in or with GSA who comes in contact with CUI is responsible for protecting and properly securing CUI, for reporting incidents, for following CUI policies and procedures, and for completing all required CUI training; and

(2) Authorized holders who create CUI or manage applications containing CUI are responsible for ensuring the proper CUI markings are applied.

9. Training.

a. All GSA employees are required to complete the awareness and training sessions commensurate with their duties.

(1) Per 32 C.F.R. § 2002, all personnel must take initial CUI awareness training within 60 days of employment, plus refresher training at least every two years thereafter. This training may be included in an existing class or a separate class, to be decided by the CUI SAO.

(2) Personnel who create and/or handle CUI on a regular basis must have a deeper knowledge and understanding of relevant CUI categories, the CUI Registry, proper markings, and applicable safeguarding/dissemination/decontrol policies and procedures, as described in GSA's CUI Guide and the CUI Registry. These employees will need additional specific training or awareness activities.

(3) Personnel who are involved in the management, design, development, operation, and use of systems that contain CUI must be knowledgeable of their responsibilities for safeguarding CUI systems and information. Additional training or awareness activities will be required of these employees.

b. Contractors must complete training as required by their specific contract. FAR Case 2017-016 (Controlled Unclassified Information) has been opened and will likely add training requirements for applicable contractors.

c. Mandatory training will be completed through GSA's Online University (OLU) or via hard copy for those without access to OLU. Additional awareness and training topics will be presented through websites, webinars, meetings, documents, or other methods as appropriate for the content.

10. Marking and Safeguarding.

a. All CUI systems and information must be protected according to applicable laws, regulations, or Government-wide policies. Specific procedures for marking are outlined in GSA's Marking Manual which can be found on the CUI InSite page. Authorized holders of CUI will be held accountable for knowing and following these procedures as described in the mandatory training and the CUI Guide. CUI shall be protected at all times in a manner that minimizes the risk of unauthorized disclosure while allowing for access by authorized holders.

b. Authorized holders of CUI are responsible for complying with applicable safeguarding requirements in accordance with 32 C.F.R. § 2002, GSA's CUI Guide, and all applicable guidance published in the CUI Registry.

c. Due to varied time spans that agencies will transition from legacy markings to CUI, some sensitive information may not be marked properly, or may not be marked at

all. This information should still be handled and safeguarded as CUI. Anyone finding an incorrectly marked document should notify the disseminating individual or agency and request a properly marked document, or have them confirm that it is not CUI.

d. For categories specifically designated as CUI Specified, holders must follow the procedures in the underlying laws, regulations, or Government-wide policies that established the specific category involved. This information is available in the CUI Registry found at archives.gov/cui.

e. CUI Banner Markings of legacy documents are not required unless the documents, files, or systems are made active again. This policy grants automatic waivers to CUI marking requirements for material that was previously marked with older markings (Sensitive But Unclassified, For Official Use Only, private, etc.), is stored in a protective manner, and is only accessible to GSA. If the information is made active again or is shared outside of GSA it must be reviewed and, if appropriate, marked as CUI. Other types of waivers are also possible; refer to the CUI Guide for details.

11. Dissemination. In accordance with 32 C.F.R. § 2002.16(a)(3), as amended, prior to disseminating CUI, authorized holders must properly label CUI. Prior to disseminating CUI to non-executive branch entities, GSA should enter into a formal agreement such as a Memorandum of Understanding or Inter-agency Agreement that includes the requirement to comply with EO 13556 and the CUI Registry. At a minimum, the agreement shall include the provisions at 32 C.F.R. § Part 2002.16(a)(6), as amended.

12. Self-Inspection. In accordance with 32 C.F.R. § 2002, GSA must maintain internal oversight efforts to measure and monitor implementation and management of the CUI Program.

a. The program must include no less than one annual periodic review and assessment of GSA's CUI program.

b. The program will be managed by the CUI PM and be implemented across GSA in coordination with assigned representatives.

c. Details of the program including requirements and procedures are maintained in the CUI Guide.

13. Misuse. Misuse of CUI occurs when someone uses CUI in a manner not in accordance with 32 C.F.R. § 2002, the CUI Registry, this policy, or the applicable laws, regulations, or Government-wide policies that govern the affected information. This may include intentional violations or unintentional errors in safeguarding or disseminating CUI. This may also include designating or marking information as CUI when it does not qualify as CUI.

a. 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.

b. Any disciplinary action within GSA shall be guided by HRM 9751.1 Maintaining Discipline.

c. Misuse of CUI must be reported to the CUI PM and is reportable to the Insider Threat Program under ADM P 2400.1A, Appendix B. See GSA's CUI Guide for further details.

14. CUI and Other Authorities.

a. CUI and the Freedom of Information Act (FOIA).

(1) CUI markings and designations are not to be used in making a determination on releasing records in response to a FOIA request. Determinations must be made according to the criteria set out in the governing law, not on the basis of the information's status as CUI.

(2) If records are released to the public pursuant to FOIA, that does not constitute decontrol and the information will remain controlled within GSA until and unless it is decontrolled.

(3) Any determination to disclose CUI in accordance with FOIA must be made after consultation with GSA's Office of General Counsel.

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

c. CUI and the Administrative Procedure Act (APA). Nothing in GSA's CUI Guide alters the Administrative Procedure Act (APA) or the powers of Federal administrative law judges (ALJs) appointed thereunder, including the power to determine confidentiality of information in proceedings over which they preside. Nor does this

impose requirements concerning the manner in which ALJs designate, disseminate, control access to, decontrol, or mark such information, or make such determinations.

d. CUI and the Privacy Act.

(1) The CUI Registry provides additional information to help determine which CUI Category and marking applies to different types of information covered by the Privacy Act. Also see the GSA Privacy Act Program or CIO 2200.1 GSA Privacy Act Program, or direct questions to the Chief Privacy Officer or the Office of General Counsel.

(2) In accordance with 32 C.F.R. § 2002, Privacy Act information is considered a subset of CUI and should be marked accordingly using one of the Privacy categories as denoted in the CUI Registry.

(3) Dissemination of CUI is permitted when in accordance with laws, regulations and Government-wide policies including the Privacy Act, and when not otherwise prohibited by law. Written agreements are not required when sharing CUI with individuals or entities when released pursuant to a Privacy Act request. See 32 C.F.R. § 2002.16 for details.

(4) This type of information shall also be handled in accordance with CIO 2180.2 GSA Rules of Behavior for Handling Personally Identifiable Information (PII).

15. References.

a. Executive Order 13556 Controlled Unclassified Information (CUI)

b. 32 Code of Federal Regulations (CFR) Section 2002

c. InSite page with link to GSA's CUI Guide

d. CIO 2100.1 GSA Information Technology (IT) Security Policy

e. CIO 2200.1 GSA Privacy Act Program

f. CIO 2104.1B GSA Information Technology (IT) General Rules of Behavior

g. CIO 2180.2 GSA Rules of Behavior for Handling Personally Identifiable Information (PII)

h. ADM P 2400.1A Insider Threat Program

i. ADM 5450.39D GSA Delegations of Authority Manual

j. PBS P 3490.3 CHGE 1 Security for Sensitive Building Information Related to Federal Buildings, Grounds, or Property

k. GSA's CUI page on InSite

l. The CUI Registry

16. Signature.

DocuSigned by:
David Shive
A3AE4284A2754F9...

DAVID SHIVE
Chief Information Officer
Office of GSA IT