



## CUI Notice 2020-01: CUI Program Implementation Deadlines

May 14, 2020

### Purpose

1. This Notice updates agency implementation deadlines for the Controlled Unclassified Information (CUI) Program. We are issuing these updated deadlines to facilitate agency coordinated transition to the CUI Program and are basing them on agency projections provided in CUI annual report submissions to the Information Security Oversight Office (ISOO).
2. This Notice rescinds:
  - a. CUI Notice 2016-01: Implementation Guidance for the Controlled Unclassified Information Program; and
  - b. CUI Notice 2018-03: Implementation and Compliance Reporting and Delays
3. This guidance document is binding on agency actions as authorized under applicable statute, executive order, regulation, or similar authority. This guidance document does not have the force and effect of law on, and is not meant to bind, the public, except as authorized by law or regulation or as incorporated into a contract.

### Authorities

4. Executive Order 13556, Controlled Unclassified Information (November 4, 2010); and
5. 32 CFR Part 2002, Controlled Unclassified Information (September 14, 2016).

### Background

6. Executive Order 13556, "Controlled Unclassified Information" (the Order), November 4, 2010, established the CUI Program to standardize the way the executive branch handles unclassified information that requires protection in accordance with law, regulation, and Government-wide policy. The Director of ISOO exercises Executive Agent (EA) responsibilities for the CUI Program. The CUI Federal regulation at 32 CFR 2002 implements the Order and establishes CUI Program requirements for safeguarding, disseminating, marking, decontrolling, and disposing of CUI. Agency policy, procedure, and practice must be modified to reflect the standards of the CUI Program.
7. The Order required that the CUI EA, in consultation with affected agencies and the Office of Management and Budget (OMB), "establish deadlines for phased implementation by agencies" (Section 5b). In consultation with OMB, on September 14, 2016, ISOO issued CUI Notice 2016-01, Implementation Guidance for the Controlled Unclassified Information Program. CUI Notice 2016-01 identified the core elements of a CUI Program, identified the

sequence of agency implementation activities, and established initial implementation deadlines.

8. On November 1, 2017, agencies submitted their first CUI annual report to ISOO. They reported significant impediments to implementation, including insufficient funding and staffing, cited by the majority of agencies as the primary cause for the delays. ISOO highlighted the issues and needs reported by agencies in its 2017 Annual Report to the President. In response to the delays and issues reported by agencies, on March 13, 2018, ISOO issued CUI Notice 2018-03, Implementation and Compliance Reporting and Delays. That Notice:
  - a. Recognized the numerous factors (an agency's size, mission, the volume of CUI handled, resource dependencies, etc.) that might delay implementation within an agency; and
  - b. Provided guidance on how an agency should report issues related to implementation.
9. Based on 2017, 2018, and 2019 agency CUI annual reports to ISOO, agencies across the executive branch have made significant progress implementing the CUI Program and meeting the previously outlined implementation phases. Most agencies project full program implementation by the end of the third quarter of FY 2021. ISOO attributes much of this progress to the leadership, initiative, and resourcefulness of senior program officials within agencies. Accordingly, in order to facilitate the next steps in the executive branch's coordinated transition to the CUI Program, we are establishing the following deadlines.

### **Implementation Deadlines**

#### **Awareness campaign**

10. By **June 30, 2020**, agencies must initiate an awareness campaign that informs their entire workforce of the coming transition to the standards of the CUI Program. This effort should:
  - a. Define CUI;
  - b. Identify or provide examples of the types of information that qualify as CUI;
  - c. Provide an introduction to CUI markings and limited dissemination controls and control markings;
  - d. Convey that, during the remaining implementation phases, existing practices for sensitive information will coexist with CUI practices and will eventually be phased out;
  - e. Summarize the agency's plans and timelines to implement the CUI Program; and
  - f. Address how to handle CUI prior to the agency's full implementation of the CUI Program and address how to re-mark or reuse legacy information (unclassified information that an agency marked as restricted from access or dissemination in some way, or otherwise controlled, prior to the CUI Program).

#### **Policy**

11. By **December 31, 2020**, agencies must issue policies that implement the CUI Program. Agencies may implement the CUI Program through a single policy or through multiple policies that address specific elements of the CUI Program. They may issue new policies

while rescinding existing ones or modify existing policies to bring their policies into compliance.

12. If an agency has sub-agencies, all those subordinate components must develop and publish implementing policies and/or modify or rescind all affected policies by June 30, 2021.
13. At a minimum, agency policies should:
  - a. Identify the office or organization designated to fulfill responsibilities for the CUI Program;
  - b. Identify by position and/or title the CUI SAO;
  - c. Identify by position and/or title the CUI PM;
  - d. Establish a system for reporting incidents involving CUI;
  - e. Establish an agency self-inspection program;
  - f. Establish training requirements for CUI Basic and Specified categories;
  - g. Address safeguarding, including marking, physical safeguarding, information system safeguarding, dissemination standards, document markings, destruction, and decontrol;
  - h. Address the unique safeguarding or handling requirements for CUI Specified categories or subcategories; and
  - i. If applicable and necessary to ensure the proper safeguarding of a category of CUI, agency CUI policies should also identify CUI categories routinely handled by agency personnel, including any safeguarding or handling requirements identified in laws, regulations, and Government-wide policies.
  - j. We strongly recommend that offices that regularly handle CUI should develop SOPs to apply and implement safeguarding, handling, marking requirements, and agency practices for those categories of CUI the office regularly handles.

### **Classification marking tools and commingling**

14. By **December 31, 2020**, agencies that manage, own, or control Classification Marking Tools (CMT) used to mark Classified National Security Information must have initiated any modification of such CMTs as necessary to begin accounting for CUI markings described on the CUI Registry and the standards described in 32 CFR 2002.20(g).
15. Agencies that depend on modification of any CMTs to achieve full CUI implementation must, in their FY 2020 annual report and each annual report thereafter:
  - a. Report such dependencies to ISOO;
  - b. Describe which implementation requirements from 32 CFR 2002 and this notice are affected by the specific CMT dependencies and provide a projected date by which you expect to be able to meet those requirements; and
  - c. Provide updates on the progress of modifications and implementation of these requirements (in particular, 32 CFR 2002.20(g)'s marking provisions) to the CUI EA.
16. CUI Notice 2018-05, Implementation Guidance when Commingling Controlled Unclassified Information (CUI) and Classified National Security Information (CNSI), provides agencies with marking guidance for commingling CUI and CNSI while they are transitioning to the CUI Program and while automated marking tools are developed or modified to meet the marking standards described in 32 CFR 2002.

## Training

17. By **December 31, 2021**, agencies (including any sub-agencies or components) must deploy CUI training to all affected employees. Agencies may implement CUI training through a single module or through multiple modules. CUI training may be incorporated into existing agency training (such as privacy, information systems, or records management training). CUI training must:
- a. Convey individual responsibilities related to protecting CUI;
  - b. Identify the categories routinely handled by agency personnel and any special handling requirements for CUI Specified;
  - c. Describe the CUI Registry and its purpose, structure, and location (i.e., <http://www.archives.gov/cui/>);
  - d. Describe the differences between CUI Basic and CUI Specified;
  - e. Identify the offices or organizations with oversight responsibilities for the CUI Program;
  - f. Address CUI marking requirements, as described by agency policy;
  - g. Address the required physical safeguards and methods for protecting CUI, as described by agency policy;
  - h. Address the destruction requirements and methods, as described by agency policy;
  - i. Address the incident reporting procedures, as described by agency policy;
  - j. Address the methods and practices for properly sharing or disseminating CUI within the agency and with external entities inside and outside of the executive branch; and
  - k. Address the methods and practices for properly decontrolling CUI, as described by agency policy.

## Physical safeguarding

18. By **December 31, 2021**, agencies (including any sub-agencies or components) must implement or verify that all physical safeguarding requirements, as described in 32 CFR 2002 and in agency policies, are in place. When CUI is not under an authorized holder's direct control, it must be protected with at least one physical barrier that provides reasonable assurance that the CUI will be protected from unauthorized access or observation. Agencies can leverage or utilize existing policies and practices when implementing this aspect of the CUI Program.
19. The physical security requirements for CUI found in 32 CFR 2002 give agencies considerable latitude to define and maintain an environment that will prevent and detect unauthorized access. After an examination of existing physical safeguarding measures, many agencies find that much of their existing physical safeguarding measures already align to the requirements found in 32 CFR 2002. Your agency can assert full implementation, for physical safeguarding, when it has completed this validation and transition.

## Information systems

20. By **December 31, 2021**, agencies (including any sub-agencies or components) must modify all Federal information systems to the standards identified in 32 CFR 2002. Federal and

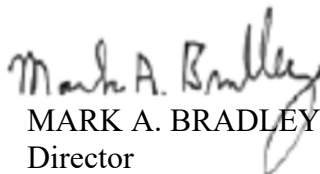
contractor information systems that are used to store, process, or transmit CUI must be configured at no less than the Moderate Confidentiality impact value (see 32 CFR 2002.14).

21. The Moderate Confidentiality impact value was established as the standard baseline due to the assertion by agencies that the majority of executive branch systems that contain privacy information are already aligned to this standard (or in some cases, the high baseline).
22. From an implementation standpoint, agencies must validate that all agency systems that store, process, or transmit CUI align to this standard and also identify any systems that contain CUI that fall below the Moderate Confidentiality impact value. Those systems that fall below this standard must be targeted for modification to this standard. Your agency can assert full implementation, for information systems, when it has completed this validation and transition for agency-reportable systems.

### **Reporting**

23. CUI Senior Agency Officials must submit an annual report on the CUI Program to ISOO no later than November 1 each year, and report on implementation during the preceding fiscal year. Reports must cover all implementation and program activities from October 1 to September 30 of the preceding fiscal year. Only parent agencies are required to report directly to ISOO. Agency components, elements, sub-agencies, regional locations, divisions, and/or internal lines of business must report to their parent agency.
24. Agencies that anticipate delays in implementing any of the above deadlines must include a narrative in their annual report submission that describes the issue giving rise to the delay and projects when they expect to implement the delayed program element. They must also include a copy of their implementation plan or strategy. ISOO will evaluate and formally approve delays on a case-by-case basis and may report such delays to the President.

**Please direct any questions regarding this notice to [CUI@nara.gov](mailto:CUI@nara.gov)**

  
MARK A. BRADLEY  
Director