INFORMATION SECURITY OVERSIGHT OFFICE
NATIONAL ARCHIVES *and* RECORDS ADMINISTRATION
700 PENNSYLVANIA AVENUE, NW, ROOM 100 WASHINGTON, DC 20408-0001
www.archives.gov/isoo

CUI Notice 2017-01: Implementation Recommendations for the Controlled Unclassified Information Program

June 12, 2017

Purpose

The purpose of this notice is to provide recommendations for agency implementation of the Controlled Unclassified Information (CUI) Program based on the 32 CFR part 2002.

Background

The Information Security Oversight Office (ISOO) exercises Executive Agent responsibilities for the CUI Program. In consultation with the Office of Management and Budget and affected agencies, on September 14, 2016, ISOO issued CUI Notice 2016-01, "Implementation Guidance for the Controlled Unclassified Information Program." CUI Notice 2016-01 outlines the phased implementation deadlines for agencies and describes the significant elements of a CUI Program.

Structure of the Notice

The attached recommendations are organized into the following sections to address programmatic elements:

I. Program Management;
II. Policy;
III. Training and Awareness;
IV. Physical Safeguarding;
V. Information Systems;
VI. Destruction;
VII. Self-Inspections;
VIII. Incident Management; and
IX. Contracts and Agreements.

Not all recommendations apply to every agency, but may serve to organize and focus implementation efforts.

Agencies are encouraged to contact the CUI staff at ISOO with any questions at: cui@nara.gov

Mark A. Bradley

MARK A. BRADLEY
Director

Attachment

Recommendations
for Agency Implementation of the Controlled Unclassified Information (CUI) Program

I. Program Management

ISOO's memorandum to the heads of executive departments and agencies, "Appointments of Senior Agency Official and Program Manager for the Controlled Unclassified Information (CUI) Program Implementation," dated April 11, 2013, requested that agencies affirm or update their initial designations of their CUI Senior Agency Official (SAO) and also requested that they assign a CUI Program Manager (PM).

1. Select a CUI SAO, assign a CUI PM and designate an organization to lead implementation efforts.

    a. CUI SAOs should represent an adequate level of authority within your agency to ensure overall program success in areas including resource acquisition, and the approval of policy, training, and self-inspection practices.

    b. CUI PMs, on behalf of the CUI SAO, interact directly and officially with ISOO on matters related to the day-to-day operations of your agency's CUI Program, including policy development, training efforts, agency self-inspection programs, information technology changes and other programmatic elements.

    c. Since the issuance of the 32 CFR part 2002, many agencies have reevaluated who should be leading the implementation efforts for their agencies.

        i. Most agencies have appointed CUI SAOs from the organization of their chief information officer, often based on the consideration that most CUI is commonly accessed through the electronic environment, and on which agency organization has the ability to cross or impact internal lines of business. As another consideration, most agencies now train their personnel on the protective measures for sensitive information using computer based training frequently developed and maintained by the chief information officer's organization.

        ii. Some agencies appoint CUI SAOs from their security organization, largely based on the expertise and methods developed within this element to manage and oversee security operations within an agency. In such cases, frequently, these agencies adapt and heavily rely on existing methods and practices used to protect Classified National Security Information as a baseline for protecting sensitive information.

    d. Factors that may be used in selecting the CUI SAO and organization to lead implementation efforts, can include:

        i. What categories or subcategories of CUI the agency handles;

ii. The medium through which the agency handles CUI, such as the electronic environment;
iii. Which office or internal organization currently oversees and manages the handling of sensitive information within the agency;
iv. Which office or internal organization serves as the existing focal point for security advice and reporting security incidents;
v. Which office or internal organization holds or will receive the resources to implement and sustain information security activities.

2. Choose other CUI leadership from within existing lines of business, component agencies, regional locations, and other major elements to implement the CUI Program.

   a. In order to adequately protect sensitive information within large and complex organizations, such officials may take on responsibilities for implementing and sustaining CUI Program requirements as part of their current duties.

3. Form a working group or body to focus specifically on implementation and sustainment activities related to the CUI Program.

   a. The agency head or CUI SAO should establish the working group either through agency correspondence or through agency policy. Membership should include all stakeholders within the agency and all internal lines of business or component organizations to include component agencies.

   b. Recommended activities for this group include:

      i. Identify all policies or procedures that prescribe protective measures for sensitive information, including everything that the agency needs to modify or rescind in implementing the CUI Program;
      ii. Identify any potential new CUI categories and subcategories;
      iii. Identify all training modules or awareness efforts that prescribe protective measures for sensitive information, including everything that the agency needs to modify or rescind in implementing the CUI Program;
      iv. Continuously identify issues that should or can be addressed through additional policy, training, or awareness initiatives.

4. Initiate a data call to the workforce in order to evaluate and compare all those information types the agency is currently protecting that cannot be linked to an existing law, regulation, and government-wide policy listed in the CUI Registry and whose continued protection is needed. Refer any gaps in protection to the CUI Executive Agent for additional analysis and guidance.

5. Develop and document an implementation strategy or plan that details all implementation activities for the agency, including any component agencies and all regional locations. At a minimum, implementation plans should include the core elements of implementation

identified by CUI Notice 2016-01 such as policy, training, physical safeguarding, systems transition, and a self-inspection program.

a. Such plans or strategies do not need to be submitted to the CUI Executive Agent for approval or as a part of the agency's report on implementation. Nevertheless, these plans can serve as a basis for the dates or milestones conveyed to the CUI Executive Agent as part of the agency's annual report.

II. Policy

Agency regulations will provide the foundation for effective management, oversight, and sustainment of program activities. Agencies may implement the CUI Program through a single policy or through multiple policies that address specific elements of the CUI Program. At a minimum, agency policies should address:

a. The CUI Registry;
b. CUI categories and subcategories;
c. Safeguarding CUI in the physical environment;
d. Safeguarding CUI in the electronic environment;
e. Access and dissemination;
f. Marking and identification;
g. Limitations on the applicability of agency policy;
h. Contracts and agreements;
i. Agency self-inspection program;
j. Education, training, and awareness;
k. Transferring records;
l. Legacy materials;
m. Waivers of CUI requirements;
n. CUI and disclosure statutes;
o. CUI and the Privacy Act;
p. Challenges to the designation of CUI; and
q. Misuse of CUI;

1. Identify all existing agency policy and procedure that prescribe protective measures for sensitive information within the agency (to include any component agencies or internal lines of business).

   Note: All policies and procedures identified must be modified to incorporate CUI Program elements, for example, identification, safeguarding, marking, sharing, destruction, and decontrol. Below is a list of common agency policies that often prescribe protective measures for sensitive information:

   a. Telework policy;
   b. Escort policy;
   c. Bring your own device policy;
   d. Continuity of operations plans;

e. Systems security policy;
f. Physical security policy;
g. Records and ascension policy;
h. Personally Identifiable Information and privacy policy; and
i. Classified National Security Information policy.

2. Assess and inventory the categories and subcategories of CUI handled within the agency, including those handled by component agencies.

3. Ensure that all prescriptive requirements found in the underlying authorities for CUI Specified categories or subcategories are reflected in applicable agency policies.

4. Ensure that agency policies reflect the elements addressed on CUI Notice 2016-01. At a minimum, agency policies should:

   a. Identify the office or organization designated to fulfill the responsibilities associated with 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; and
   g. Address safeguarding, including marking, physical safeguarding, dissemination standards, document markings, destruction, and decontrol.
   h. Address the unique safeguarding or handling requirements for CUI Specified categories or subcategories.
   i. If applicable and necessary to ensure the proper safeguarding of a category or subcategory of CUI, agency CUI policies may also identify all CUI routinely handled by agency personnel.

III. Training and Awareness

Proactive education and training are major elements of an effective security program. Personnel who handle and/or create sensitive information must maintain a satisfactory knowledge and understanding of the protective measures that prevent or deter disclosures to unauthorized persons.

1. Identify all existing agency training modules or awareness products that prescribe protective measures for sensitive information within the agency, including any component agencies or internal lines of business.

   Note: Training modules or awareness products identified must be modified to incorporate CUI Program elements such as identification, safeguarding, marking, sharing, destruction, and decontrol. Agency training or awareness products that often prescribe protective measures for sensitive information include:

a. Telework training;
b. Systems security awareness training;
c. General physical security;
d. Records management training;
e. Personally Identifiable Information and privacy training; and
f. Classified National Security Information training.

2. Raise awareness or inform the workforce about the transition to the CUI Program and about its key elements through newsletters or email "blasts." Many agencies use a number of electronic newsletters or email "blasts" to raise awareness about various information security issues and to inform personnel about agency programs and efforts. These newsletters and emails can address the following CUI Program elements:

   a. What the reporting procedures and requirements are for incidents involving CUI;
   b. How to securely telework with CUI;
   c. How to identify a controlled environment;
   d. How to remark 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); and
   e. How to handle CUI prior to an agency's full implementation of the CUI Program.

3. Incorporate CUI training elements into existing required courses when possible. It is likely that all personnel, including contractors, with access to CUI will require some form of training. Since existing courses already address the protection of sensitive information on some level, it may be advisable to incorporate training elements into existing courses rather than to create a new training module. The CUI training requirement should be identified in all relevant agency policies.

4. Develop a webpage dedicated to the CUI Program. This page may be used to provide a general overview of the program, links to or information about CUI training courses, links to coversheets or agency policies, and information regarding when the agency will begin to implement the CUI Program. The site could also provide contact information for the CUI PM and SAO.

5. Consider developing at least four types of training:

   a. Awareness training. Awareness training or efforts will acquaint their workforce with the coming transition to the CUI Program within their agency and throughout the executive branch. The CUI Program will occur in phases, meaning that each agency of the executive branch will implement the program at their own pace (based on funding, resources, and individual timelines found in implementation plans) and that during this period both CUI and legacy information may exist at the same time. It may also be possible for one agency to implement the CUI Program ahead of others; employees should be made aware of this possibility and be informed as to how to handle both CUI and legacy information.

Note: This training is not required, but highly recommended. This training may include:

i. The reasons why the executive branch is moving to the CUI Program;
ii. Summary of information security incidents that led to the transition to the CUI Program;
iii. Definition of CUI;
iv. Description of the CUI Registry:
v. Introduction to CUI markings and how to identify CUI;
vi. Summary of the agency's implementation plans and timelines to implement the CUI program; and
vii. How to handle CUI prior to the agency's full implementation of the CUI Program;

b. Orientation training. Orientation training will acquaint the workforce with the agency's CUI policy and program. Following CUI Notice 2016-01, at a minimum, this training must:

i. Convey individual responsibilities related to protecting CUI;
ii. Identify the categories or subcategories routinely handled by agency personnel and any special handling requirements for CUI Specified;
iii. Describe the CUI Registry and its purpose, structure, and location (i.e., http://www.archives.gov/cui/);
iv. Describe the differences between CUI Basic and CUI Specified;
v. Identify the offices or organizations with oversight responsibilities for the CUI Program;
vi. Address CUI marking requirements, as described by agency policy;
vii. Address the required physical safeguards and methods for protecting CUI, as described by agency policy;
viii. Address the destruction requirements and methods, as described by agency policy;
ix. Address the incident reporting procedures, as described by agency policy;
x. 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
xi. Address the methods and practices for properly decontrolling CUI, as described by agency policy.

c. Specified training. Specified training will acquaint the workforce or a portion of the workforce with the special or unique handling requirements for CUI Specified categories or subcategories. An agency, depending on mission and internal structure, may have multiple Specified training modules in place. Recommend that agencies identify employees, job series, or roles that handle those categories of CUI that require special handling or safeguarding requirements as described in law, regulation, or government-wide policy, and develop or identify training modules that address these requirements.

Note: Not all employees will or should have to take specialized training. Most agencies already have some sort of training or awareness program in place to address the specific requirements called for in the underlying laws, regulations, and government-wide

policies that relate to the information, for example, privacy training; such modules or products must be modified to address the elements of the CUI Program that apply.

d. Refresher training. Refresher training reacquaints the workforce with safeguarding principles addressed in the initial orientation training. This training must be administered, at a minimum, every two years.

IV. Physical Safeguarding

CUI must be protected in electronic and physical environments. 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. A controlled environment is any area or space that has adequate physical or procedural controls to protect CUI from unauthorized access or disclosure.

The 32 CFR part 2002 allows for considerable flexibility when it comes to ensuring that CUI is adequately protected in the physical environment. Agencies can leverage or utilize existing policies and practices when implementing the CUI Program.

For example, most agencies afford sensitive information (or CUI) with a level of physical protection that already meets or exceeds the requirements identified within the 32 CFR part 2002. Through their efforts to implement Homeland Security Presidential Directive 12, most agencies have also already taken steps to establish "controlled environments" by limiting access to select areas using the security features of the Common Access Card. In addition, most agencies have physical security policies and programs in place that establish a baseline for ensuring physical security within an agency or sub-agency, at all regional locations. These programs and policies routinely establish the "escort" policy within agencies and the incident reporting procedures or guidelines for when unauthorized individuals are found within controlled working environments.

1. Evaluate the protective measures, policies, and procedures currently used within and across the agency to protect facilities, assets, and working environments to ensure that:

   a. The protective measures currently used are sufficient to prevent the unauthorized access of CUI;
   b. The protective measures or standards are reflected in some sort of agency policy or procedure;
   c. The protective measures or standards are implemented throughout the agency (to include component agencies or internal lines of business); and
   d. That a system is in place or will be in place, as part of the implementation of the CUI Program, to routinely evaluate and ensure the implementation of the protective measures.

2. Assess the workforce and the physical workspaces to ensure that unauthorized access or opportunities for access are not afforded to those without a lawful government purpose. Individuals or work units who are working with certain types of CUI might need to be

segregated from other parts of the workforce to ensure unauthorized access or disclosure does not occur. Ensure that:

a. Employees know which areas or work environments are acceptable for storing, handling, and discussing CUI;
b. CUI is stored in an environment that includes at least one physical barrier of protection that would show evidence of tampering or alteration. When appropriate, provide employees with areas, offices, cabinets, or drawers where CUI may be stored.

V. Information Systems

Information systems that used to store, process, or transmit CUI must be configured at no less than the Moderate Confidentiality impact value (see 32 CFR part 2002.14). The majority of the systems throughout the Executive branch are already configured to this standard.

1. Identify all information systems used to store, process, or transmit CUI;
2. Assess or determine their current configuration; and
3. Develop a plan or strategy to transition all information systems found to be configured lower than Moderate Confidentiality.

VI. Destruction

When destroying CUI, including in electronic form, agencies must do so in a manner that makes the media unreadable, indecipherable, and irrecoverable. Agencies must use any destruction method specifically required by law, regulation, or government-wide policy for that CUI. The National Institute of Standards and Technology Special Publication 800-88, "Guidelines for Media Sanitization," provides agencies with recommendations on how CUI can be destroyed or sanitized. Agencies should:

1. Assess the methods currently used to destroy or sanitize CUI, regardless of media, and across the agency, including component agencies or internal lines of business;
2. Identify any current policy or procedures within the agency that require a particular method of destruction or sanitization for sensitive information;
3. Identify all destruction equipment, procedures, and methods, approved and not approved for CUI destruction or sanitization; and
4. Establish a system to routinely evaluate and assess the destruction equipment, procedures, and methods used for the destruction or sanitization of CUI.

VII. Self-Inspections

Each year, agencies must conduct a review and assessment of their agency's CUI Program to evaluate program effectiveness, to measure the level of compliance, and to monitor implementation efforts.

Some agencies that conduct self-inspections operate decentralized, compartmented, and infrequent inspection programs, often limited in scope to either physical or systems protections,

and rarely performed on a regular basis to cover the entire scope of an information security program.

1. Ensure self-inspection programs evaluate all agency CUI policies and procedures; training and awareness efforts; and controlled environments or areas where CUI is stored, handled, or processed.

VIII. Incident Management

A key element of the CUI program, incident reporting includes the tracking and analysis of trends/patterns, as well as reporting the possible loss or compromise of CUI, and the response to possible losses or compromises. Incident reporting and the information that comes from tracking the types and numbers of incidents helps to influence policy changes, training updates, and the targets of self-inspection.

At present, the incident reporting systems of some agencies only focus on certain types of sensitive unclassified information, typically on privacy information, in addition to physical security issues, and the loss of any information technology equipment and the loss or compromise of classified information, wherever it is handled. However, incident reporting systems rarely integrate these monitoring activities, or include CUI (other than privacy information) within their scope.

1. Conduct internal audits of any incidents involving sensitive and privacy information and adjust training and awareness programs accordingly. Security and management personnel may benefit from an analysis of such incidents.

2. Develop mechanisms for employees to report the mishandling or misuse of CUI. Include these reporting mechanisms in any applicable training courses and standard awareness activities.

IX. Contracts and Agreements.

Agencies routinely enter into contracts and agreements with non-Federal entities or other executive branch agencies. These agreements typically contain language that in some way speaks to or calls for the protection of sensitive information.

1. Identify all contracts or agreements where safeguarding or handling guidance is conveyed for CUI; and
2. Modify all such contracts or agreements to align to the safeguarding requirements of the CUI Program (32 CFR part 2002.14).