Controlled Unclassified Information

Executive Order 13556

Shared • Standardized • Transparent

Information Security Oversight Office (ISOO)
Briefing Outline

- Executive Order 13556
- 32CFR2002 (implementing directive)
- Approach to Contractor Environment
- Phased Implementation
- Understanding the CUI Program
Why is the CUI Program necessary?

Executive departments and agencies apply their own ad-hoc policies and markings to unclassified information that requires safeguarding or dissemination controls, resulting in:

| An inefficient patchwork system with more than 100 different policies and markings across the executive branch | Inconsistent marking and safeguarding of documents | Unclear or unnecessarily restrictive dissemination policies | Impediments to authorized information sharing |

---

3
Executive Order 13556

- Established CUI Program
  - In consultation with affected agencies (CUI Advisory Council)

- Designated an Executive Agent (EA) to implement the E.O. and oversee department and agency actions to ensure compliance.
  - National Archives and Records Administration
  - Information Security Oversight Office

- An open and uniform program to manage all unclassified information within the executive branch that requires safeguarding and dissemination controls as required by law, regulation, and Government-wide policy
EO 13556 called for a review of the categories, subcategories, and markings currently used by agencies.

Agencies submitted over 2,200 authorities for controlling many types of information.

Information types were grouped together, legal authorities were examined, and a CUI Registry was published.

- 23 Categories
- 84 Sub-categories
- 315 Control citations
- 106 Sanction citations
Implements the CUI Program

- Establishes policy for designating, handling, and decontrolling information that qualifies as CUI
  - Effective: November 14, 2016 (Day 0)

Describes, defines, and provides guidance on the minimum protections (derived from existing agency practices) for CUI

- Physical and Electronic Environments
- Marking
- Sharing
- Destruction
- Decontrol

Emphasizes unique protections described in law, regulation, and/or Government-wide policies (authorities)
• Agencies must use NIST SP 800-171 when establishing security requirements to protect CUI’s confidentiality on non-Federal information systems.

• The NIST 800-171 is intended for use by federal agencies in appropriate contractual vehicles or other agreements established between those agencies and nonfederal organizations.

• Establishes requirements for protecting CUI at the Moderate Confidentiality Impact Value.

• Non-tailorable requirements

• Flexibility in how to meet requirements
When to use the NIST SP 800-171

- **Use the NIST SP 800-171 when a non-Federal entity:**
  - Receives CUI incidental to providing a service or product to the Government outside or processing services. Examples: producing a study, conducting research, creating a training program, building an aircraft or ship, etc.
  - In these instances, the Government is only concerned with the confidentiality of the information and the CUI is regarded as the asset requiring protection.

- **Do NOT use the NIST SP 800-171 when a non-Federal entity:**
  - Collects or maintains CUI as part of a Government function (e.g., census takers or records storage).
  - Builds an information system or operates an information system for the Government (an email provider, or payroll system).
  - Provides processing services for the Government (a cloud service provider).
  - In these instances, the Government has a concern in the confidentiality, integrity, and availability of the information system and the system is the asset requiring protection.
  - Agencies may require these systems to meet additional requirements the agency sets for its own internal systems.
To promote standardization, the CUI Executive Agent plans to sponsor a Federal Acquisition Regulation (FAR) clause that will apply the requirements contained in the 32 CFR Part 2002 and NIST SP 800-171 to industry.
Implementation of the CUI Program

Day 0 (14 Nov ‘16) 180 Year 1 180 Year 2

Policy
- Develop and Publish Policy
- Develop and Publish Component Policy

Training
- (Planning)
- Develop and Deploy Training
- Complete CUI Training

Physical Safeguarding
- (Planning)
- Implement Physical Safeguarding

Systems
- Assessment of Systems
- Develop Systems Transition Strategy

Self-Inspection
- Initiate Internal Oversight

180 Year 1
- Transition Strategy

180 Year 2
- Oversight

Day 0 (14 Nov ‘16)
-启动

180 Year 1
- 发展和部署培训
- 完成 CUI 培训

180 Year 2
- 内部监督
Additional Implementation Concerns

- **Program Management**
  - Senior Agency Official, Program Manager, internal planning teams

- **Incident Management**
  - Reporting, Mitigation, and Preventing Recurrence

- **Contracts & Agreements (agencies and non-federals)**
  - Guidance given to external entities on how to handle CUI
  - Limitations on Applicability of Agency Policies
Understanding the CUI Program

- CUI Basic versus CUI Specified
- Limitations of Agency Policy
- Controlled Environments
- Systems Requirements: Moderate

Marking CUI
- Banner, Designator, Specified, Portion, Limited Dissemination Control Markings
- Bulk & Systems (splash screens)
- Legacy Information, derivative use.
- Handbook & Coversheets

- Destruction
Two types of CUI: Basic and Specified

- **CUI Basic** = LRGWP identifies an information type and says protect it.

  **Examples include:** Agriculture, Ammonium Nitrate, Water Assessments, Emergency Management, Bank Secrecy, Budget, Comptroller General, Geodetic Product Information, Asylee, Visas, Information Systems Vulnerabilities, Terrorist Screening, Informant, Privilege, Victim, Death Records

- **CUI Specified** = LRGWP identifies an information type and says to protect it, and also includes one or more specific handling standards for that information.

  **Examples include:** Sensitive Security Information, Student Records, Personnel, Source Selection, Nuclear, Safeguards Information, NATO Restricted, NATO Unclassified, Federal Grand Jury, Witness Protection, DNA, Criminal History Records, Financial Records, Export Control, Protected Critical Infrastructure Information, Controlled Technical Information
Limitations on applicability of agency CUI policies

- Agency policies pertaining to CUI do not apply to entities outside that agency unless the CUI Executive Agent approves their application and publishes them in the CUI Registry.

- Agencies may not levy any requirements in addition to those contained in the Order, this Part, or the CUI Registry when entering into contracts, treaties, or other agreements about handling CUI by entities outside of that agency.
Agencies must safeguard CUI at all times in a manner that minimizes the risk of unauthorized disclosure while allowing for access by authorized holders.

- For categories designated as CUI Specified, personnel must also follow the procedures in the underlying law, regulation, or Government-wide policy that established the specific category or subcategory involved.

Safeguarding measures that are authorized or accredited for classified information are sufficient for safeguarding CUI.
Controlled environment is any area or space an authorized holder deems to have adequate physical or procedural controls (e.g., barriers and managed access controls) for protecting CUI from unauthorized access or disclosure.

- When outside a controlled environment, you must keep the CUI under your direct control or protect it with at least one physical barrier. You or the physical barrier must reasonably protect the CUI from unauthorized access or observation.
System Requirements: Moderate

- Systems that store or process CUI must be protected at the Moderate Confidentiality Impact Value.
  - FIPS PUB 199 & 200
  - NIST SP-800-53 (Risk Based Tailoring)

- Moderate = The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. (FIPS PUB 199)
  - A serious adverse effect means that, for example, the loss of confidentiality might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries
Agencies must uniformly and conspicuously apply CUI markings to all CUI prior to disseminating it unless otherwise specifically permitted by the CUI Executive Agent.

The CUI banner marking must appear, at a minimum, at the top center of each page containing CUI.
The CUI Banner Marking may include up to three elements:

- The CUI Control Marking (mandatory) may consist of either the word “CONTROLLED” or the acronym “CUI.”

- CUI Category or Subcategory Markings (mandatory for CUI Specified). CUI Control Markings and Category Markings are separated by two forward slashes (/\). When including multiple categories or subcategories in a Banner Marking they are separated by a single forward slash (/).

- Limited Dissemination Control Markings. CUI Control Markings and Category Markings are separated from Limited Dissemination Controls Markings by a double forward slash (\//).
Agencies may authorize or require the use of alternate CUI indicators on IT systems, websites, browsers, or databases through agency CUI policy. These may be used to alert users of the presence of CUI where use of markings has been waived by the agency head.
In the CUI Registry, if the authority that relates to the information is indicated to be specified, documents must be marked to indicate that CUI Specified is present in the document.

Add “SP-” before any category/subcategory markings where the authority is followed by an asterisk.
June 27, 2013
MEMORANDUM FOR THE DIRECTOR
From: John E. Doe, Chief Division 5
Subject: Examples

We support the President by ensuring that the Government protects and provides proper access to information to advance the national and public interest.

We lead efforts to standardize and assess the management of classified and controlled unclassified information through oversight, policy development, guidance, education, and reporting.

“SP-” Indicates that an authority contains specific safeguarding or dissemination measures.

Recipients are encouraged to reference the underlying, “specified,” authority(s) for specific handling guidance.
Legacy Information and Markings

Legacy Information is unclassified information that an agency marked as restricted from access or dissemination in some way, or otherwise controlled, prior to the CUI Program.

All legacy information is not automatically CUI. Agencies must examine and determine what legacy information qualifies as CUI.

Discontinue all use of legacy markings.

CUI/SP-SPECIFIED//DISSEMINATION

Department of Good Works
Washington, D.C. 20006

August 27, 2016

MEMORANDUM FOR THE DIRECTOR

From: John E. Doe, Chief Division 5

Subject: Examples

We support the President by ensuring that the Government protects and provides proper access to information to advance the national and public interest.

We lead efforts to standardize and assess the management of classified and controlled unclassified information through oversight, policy development, guidance, education, and reporting.
When destroying CUI, including in electronic form, you must do so in a manner that makes it unreadable, indecipherable, and irrecoverable, using any of the following:

- Guidance for destruction in NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, and NIST SP 800-88, Guidelines for Media Sanitization;
- Any method of destruction approved for Classified National Security Information;
- Any specific destruction methods required by law, regulation, or Government-wide policy for that item.