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:

<table>
<thead>
<tr>
<th>An inefficient patchwork system with more than 100 different policies and markings across the executive branch</th>
<th>Inconsistent marking and safeguarding of documents</th>
<th>Unclear or unnecessarily restrictive dissemination policies</th>
<th>Impediments to authorized information sharing</th>
</tr>
</thead>
</table>

---

---

---

---
What are the benefits of the CUI Program?

One uniform, shared, and transparent system for safeguarding and disseminating CUI that:

- Establishes common understanding of CUI control
- Promotes information sharing
- Reinforces existing legislation and regulations
- Clarifies difference between CUI controls and FOIA exemptions
Executive Order 13556

- Established CUI Program

- Executive Agent (EA) to implement the E.O. and oversee department and agency actions to ensure compliance

- 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
Where do we begin? Define the world of CUI

- EO 13556 called for a review of the categories, subcategories, and markings currently used by agencies to control unclassified information.
  - Agencies submitted to the CUI Executive Agent what they were protecting and the basis for that protection
  - Over 2,200 submissions were received
  - Information types were grouped together, legal authorities were examined, and a CUI Registry was published.
<table>
<thead>
<tr>
<th>23 Categories</th>
<th>84 Subcategories</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agriculture</td>
<td>Legal</td>
</tr>
<tr>
<td>Controlled Technical Information</td>
<td>North Atlantic Treaty Organization (NATO)</td>
</tr>
<tr>
<td>Critical Infrastructure</td>
<td>Nuclear</td>
</tr>
<tr>
<td>Emergency Management</td>
<td>Patent</td>
</tr>
<tr>
<td>Export Control</td>
<td>Privacy</td>
</tr>
<tr>
<td>Financial</td>
<td>Procurement and Acquisition</td>
</tr>
<tr>
<td>Geodetic Product Information</td>
<td>Proprietary Business Information</td>
</tr>
<tr>
<td>Immigration</td>
<td>SAFETY Act Information</td>
</tr>
<tr>
<td>Information Systems Vulnerability Information</td>
<td>Statistical</td>
</tr>
<tr>
<td>International Agreements</td>
<td>Tax</td>
</tr>
<tr>
<td>Intelligence</td>
<td>Transportation</td>
</tr>
<tr>
<td>Law Enforcement</td>
<td></td>
</tr>
</tbody>
</table>

**Information related to proceedings in judicial or quasi-judicial settings.**

**Subcategories:**
- Administrative Proceedings*
- Collective Bargaining
- Federal Grand Jury*
- Privilege
- Witness Protection*

**Refers to personal information, or, in some cases, “personally identifiable information,” as defined in OMB-M-07-16, or “means of identification” as defined in 18 USC 1028(d)(7).**

**Subcategories:**
- Contract Use
- Death Records
- Genetic Information*
- Health Information*
- Inspector General*
- Military
- Personnel*
- Student Records*
Online Registry

http://www.archives.gov/cui

- 23 Categories
- 84 Sub-categories
- 315 Control citations
- 106 Sanction citations

Established by Executive Order 13556, the Controlled Unclassified Information (CUI) program standardizes the way the Executive branch handles unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies. Learn About CUI →

Registry

The CUI Registry is the authoritative source for guidance regarding CUI policies and practices.

Search the Registry: [ ] Go

Access Registry by
- Category-Subcategory

Policy and Guidance
- Executive Order 13556
- CUI Notices
- Additional Information
- CUI Glossary

Training

Learn about training developed by the Executive Agent for CUI users
- CUI Training Modules

Oversight

Learn about CUI oversight requirements and tools.
- CUI Reports
One uniform and consistent policy applied to a defined and organized body of information
Implements the CUI Program
- Establishes policy for designating, handling, and decontrolling information that qualifies as CUI

Describes, defines, and provides guidance on the minimum protections for CUI
- Physical and Electronic Environments
- Destruction
- Marking
- Sharing

Emphasizes unique protections described in law, regulation, and/or Government-wide policies (authorities)
- These protections must continue as described in the underlying authorities.
CUI Basic versus CUI Specified

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

- **CUI Specified = LRGWP identifies an information type and says protect it but specifies exactly how to should be protected or handled.**
Implementation Activities within Executive Branch

Day 0
- Policy
  - Develop and Publish Policy

180
- Training
  - Develop and Publish Component Policy

- Physical Safeguarding
  - Develop and Deploy Training
  - Implement Physical Safeguarding

Year 1
- Systems
  - Assessment of Systems
  - Develop Systems Transition Strategy

180
- Self-Inspection

Year 2
- Initiate Internal Oversight
This publication provides federal agencies with recommended requirements for protecting the confidentiality of CUI:

(i) when the CUI is resident in nonfederal information systems and organizations;
(ii) when the information systems where the CUI resides are not used or operated by contractors of federal agencies or other organizations on behalf of those agencies; and
(iii) where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or government-wide policy for the CUI category or subcategory listed in the CUI Registry.

The requirements apply to all components of nonfederal information systems and organizations that process, store, or transmit CUI, or provide security protection for such components.
The basic security requirements are obtained from FIPS Publication 200, which provides the high-level and fundamental security requirements for federal information and information systems.

The derived security requirements, which supplement the basic security requirements, are taken from the security controls in NIST Special Publication 800-53.

Starting with the FIPS Publication 200 security requirements and the security controls in the **moderate baseline** (i.e., the minimum level of protection required for CUI in federal information systems and organizations), the requirements and controls are tailored to eliminate requirements, controls, or parts of controls that are:

1. Uniquely federal (i.e., primarily the responsibility of the federal government);
2. Not directly related to protecting the confidentiality of CUI; or
3. Expected to be routinely satisfied by nonfederal organizations without specification.
Until the formal process of establishing a single FAR clause takes place, the CUI requirements in NIST SP 800-171 may be referenced in federal contracts consistent with federal law and regulatory requirements.