Controlled Unclassified Information
Executive Order 13556
Shared • Standardized • Transparent

Information Security Oversight Office (ISOO)
Briefing Outline

- Overview of the CUI Program
  - Establishment of the Program
  - Elements of the CUI Executive Order
  - Categories and Registry
  - Handling CUI
  - Current Efforts
  - Implementation Plan

- CUI and IT Implementation
  - CUI and NIST Standards and Guidelines
  - Publication Delivery Vehicle
Overview of the CUI Program

Controlled Unclassified Information Program

Shared • Standardized • Transparent
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 |

---

**Controlled Unclassified Information Program**

Shared • Standardized • Transparent
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
# Approved CUI Categories

<table>
<thead>
<tr>
<th>22 Categories</th>
<th>85 Subcategories</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Agriculture</td>
<td>• Bank Secrecy</td>
</tr>
<tr>
<td></td>
<td>• DNA</td>
</tr>
<tr>
<td></td>
<td>• Investigation</td>
</tr>
<tr>
<td>2. Copyright</td>
<td>12. Law Enforcement</td>
</tr>
<tr>
<td></td>
<td>13. Legal</td>
</tr>
<tr>
<td>3. Critical Infrastructure</td>
<td>14. NATO</td>
</tr>
<tr>
<td>5. Export Control</td>
<td>16. Patent</td>
</tr>
<tr>
<td>6. Financial</td>
<td>17. Privacy</td>
</tr>
<tr>
<td>7. Foreign Government</td>
<td>18. Proprietary</td>
</tr>
<tr>
<td>11. Intelligence</td>
<td>22. Transportation</td>
</tr>
<tr>
<td></td>
<td>• Financial</td>
</tr>
<tr>
<td></td>
<td>• Health Information</td>
</tr>
<tr>
<td></td>
<td>• Personnel</td>
</tr>
<tr>
<td></td>
<td>• Census</td>
</tr>
<tr>
<td></td>
<td>• Investment Survey</td>
</tr>
</tbody>
</table>
Comprised of Program Managers from the following:

Executive Office of the President (elements)
General Services Administration (GSA)
Social Security Administration (SSA)
Environmental Protection Agency (EPA)
Department of the Interior (DOI)
Nuclear Regulatory Commission (NRC)
Department of Transportation (DOT)
Department of Labor (DOL)
Department of the Treasury
Department of Housing and Urban Development (HUD)
National Science Foundation (NSF)
Department of Homeland Security (DHS)
Central Intelligence Agency (CIA)
Department of Agriculture (USDA)

Department of Commerce (DOC)
Department of Justice (DOJ)
Federal Bureau of Investigation (FBI)
National Aeronautics and Space Administration (NASA)
Department of State (DOS)
Office of the Director of National Intelligence
United States Agency for International Development (USAID)
Office of Personnel Management (OPM)
Department of Veterans Affairs (VA)
Department of Education (ED)
Department of Defense (DOD)
Department of Health and Human Services (HHS)
Department of Energy (DOE)
Office of Management and Budget (OMB)

President’s Cabinet, Chief Financial Officers (CFO) Council member agencies, major stakeholder constituent elements (CIA and FBI), and participants
Handling CUI

One uniform and consistent policy applied to a defined and organized body of information.
## Projected CUI Policy Timeline

**as of 23 May 2014**

<table>
<thead>
<tr>
<th>Proposed to Final Rule</th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feb</td>
<td>Mar</td>
<td>Apr</td>
</tr>
</tbody>
</table>

### OMB
- **May 20:** OMB tasking issued
- **June 6:** Comments Due
- **OIRA Review: Proposed Rule Stage**
- **OIRA Review: Final Rule Stage**

### EA
- Federal Rule Formatting
- NGC & COO Review
- **Public Comment**
- **EA Adjudication**
- **Archivist Review**
- **Publish Proposed Rule**
- **Prepare Final Rule**
- **Archivist Review**
- **CFR Published**
- **CFR Effective**
Job Aids for All Users

- Marking Handbook
- Safeguarding Handbook
- Category Specific Guidance
- Cover Sheets
- Awareness Posters
- Training Materials
CUI Executive Agent Current Efforts

- Maintain Registry
  - Approve additional CUI categories and subcategories based on agency submissions
  - Provide guidance on provisional approval process for new CUI categories

- Finalize CUI Policy
  - Undergoing formal OMB comment process
  - To be published in CFR

- National Implementation Plan (NIP)
  - With agencies, create and execute implementation planning framework, including deadlines for phased implementation
Five Programmatic Areas of Implementation Plan

**Governance**
The CUI Executive Agent in consultation with affected agencies manages the implementation and sustainment of the CUI Program.

**Policy and Guidance**
CUI is safeguarded, disseminated, marked and decontrolled consistent with Executive Order 13556 and implementation guidance.

**Training**
Affected personnel receive baseline training that incorporates the essentials of the CUI program and specific agency needs.

**Technology**
The security and criticality of CUI are protected by the standards and guidelines established for Federal information systems.

**Accountability**
The CUI Executive Agent and all affected agencies are accountable for improvement of the CUI program through management and oversight responsibilities.
## CUI Phased Implementation

### Phases
- **Planning**
  - Identify and initiate planning activities for CUI implementation
- **Readiness**
  - Prepare environment and workforce for the CUI transition
- **Initiation**
  - Begin implementation of CUI practices
- **Final**
  - Full Implementation of the CUI program

### Key EA Activities
- **Day 0 (FY15)**
  - Publish 32 CFR Part 2002 Rule & Supplemental Guidance (Day 0)
  - Augment Registry
  - Provide Awareness Materials & Products
  - Consult with OMB & Provide Budget Guidance
  - Review Agency Policies
- **Day 180 (FY16)**
  - Publish CUI Training (Day 180)
  - Provide Additional Guidance as needed
  - Establish Schedule for On-site Reviews
  - Provide Training Support & Consultation
- **Year 1 (FY16)**
  - Oversee Executive Branch Implementation
  - Resolve Disputes & Complaints
  - Initiate On-site Reviews
- **Year 3-4 (FY18-19)**
  - Oversee Executive Branch Implementation
  - Collect Reporting Data

### Key DIA Activities
- **Day 0 (FY15)**
  - Assert Physical Safeguarding*
  - Conduct Training*
  - Continue Budget Cycle Planning
  - Prepare IT Transition
- **Day 180 (FY16)**
  - Initiate CUI Implementation
  - Handle
  - Recognize
  - Receive
- **Year 1 (FY16)**
  - Initiate IT Transition
  - Permit Creation of CUI
  - Initiate Self-Inspection Program
- **Year 3-4 (FY18-19)**
  - Eliminate Old Markings
  - Assure use of only New Markings
  - Complete IT Transition
  - Monitor & Report Implementation

### Monitor & Report on Phased Implementation

*Required for IOC

As of 5/15/14
“This order shall be implemented in a manner consistent with...applicable Government-wide standards and guidelines issued by the National Institute of Standards and Technology, and applicable policies established by the Office of Management and Budget”, Section 6(a)3, Executive Order 13556.

Future CUI guidance where it addresses IT issues, must be aligned to Federal policies.
CUI and NIST Standards/Guidelines

- ISOO and NIST developed a strong partnership.

- “In accordance with Federal Information Processing Standards (FIPS) Publication 199, the Confidentiality impact level for CUI shall be no lower than the Moderate level” (proposed CUI rule).
  - ISOO is collaborating with NIST on developing a Publication to represent the technical standards and guidelines for Moderate Confidentiality in the contractor environment.
  - A future Federal Acquisition Rule will be the appropriate instrument for the application of these standards and guidelines.
- Appropriately tailored security control baseline for Moderate Confidentiality based on applicability to the contractor environment of operations.

- Requirement descriptions based on FIPS Publication 200 with specified understandings of the Moderate Confidentiality Impact level for protection of CUI for the contractor environment.
  - Descriptions will allow for the use of compensating security controls, namely those providing equivalent or comparable protection.

- Document development will follow standard NIST processes involving comment from public – to include industry.
CUI and NIST Guidelines

- CUI categories and subcategories will be incorporated as information types into the next revision of the NIST Special Publication 800-60, where the work of the CUI Executive Agent will be integrated.
  - The NIST SP 800-60 will reflect Moderate Confidentiality for all CUI categories and subcategories.
  - The assignment of Integrity and Availability security impact levels will follow standard NIST processes.
CUI Phased Implementation - FAR & NIST

April 2014

Day 0: FY 15

6 Months: FY16

Year 1

Year 3 - 4: FY18-19

Phases

Development

- Develop CUI Program Elements and Timeline
- Collaborate with NIST on Development of Standards for Industry

Planning

- Conduct Planning Activities for Implementation
- Collaborate with the FAR Council on Development of the FAR

Readiness

- Prepare Environment and Workforce for the CUI Transition

Initiation

- Begin Implementation of CUI Practices
- Begin Phase Out of Obsolete Practices

Final

- Full Implementation of the CUI Program

Initial Operating Capability (IOC)

Full Operating Capability (FOC)

Federal Acquisition Regulation (FAR) Development

NIST Standards and Guidelines for Industry

NIST

FAR
Contact Information

Information Security Oversight Office
Attn: CUI Program
National Archives and Records Administration
700 Pennsylvania Avenue, N.W., Room 100
Washington, DC 20408-0001

(202) 357-6870 (voice)
(202) 357-6871/6872 (fax)
cui@nara.gov
www.archives.gov/cui