Briefing Outline

- ISOO Overview
- Overview of the CUI Program
- CUI and IT Implementation
  - CUI and NIST Standards and Guidelines
  - NIST SP 800-171
- CUI Approach for the Contractor Environment
  - FAR Rule
What is the Information Security and Oversight Office?

- Oversee the Executive Branch’s system for classifying, safeguarding, and declassifying classified information
- Located at the National Archives, but receive policy guidance from the National Security Advisor
- Director appointed by the Archivist of the United States with the approval of the President
- Primary responsibilities. We administer:
  - E.O. 13526, “Classified National Security Information”
  - E.O. 13556, “Controlled Unclassified Information”
  - E.O. 13549, “Classified National Security Information Program for State, Local, Tribal and Private Sector Entities”
  - E.O. 13587 Senior Info Sharing/Safeguarding Steering Committee
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 |
What are the benefits of the CUI Program?

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

<table>
<thead>
<tr>
<th>Establishes common understanding of CUI control</th>
<th>Promotes information sharing</th>
<th>Reinforces existing legislation and regulations</th>
<th>Clarifies difference between CUI controls and FOIA exemptions</th>
</tr>
</thead>
</table>

---

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>23 Categories</th>
<th>82 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>Foreign Government Information</td>
<td>Proprietary Business Information</td>
</tr>
<tr>
<td>Geodetic Product Information</td>
<td>SAFETY Act Information</td>
</tr>
<tr>
<td>Immigration</td>
<td>Statistical</td>
</tr>
<tr>
<td>Information Systems Vulnerability</td>
<td>Tax</td>
</tr>
<tr>
<td>Information</td>
<td></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

- 23 Categories
- 82 Subcategories
- 315 unique Control citations
- 106 unique Sanction citations

http://www.archives.gov/cui
Handling CUI

One uniform and consistent policy applied to a defined and organized body of information
## Phased Implementation

### Key EA Activities

<table>
<thead>
<tr>
<th>Planning</th>
<th>Readiness</th>
<th>Initiation</th>
<th>Final</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify and initiate planning activities for CUI implementation</td>
<td>Prepare environment and workforce for the CUI transition</td>
<td>Begin implementation of CUI practices</td>
<td>Full Implementation of the CUI program</td>
</tr>
<tr>
<td>• Publish 32 CFR Part 2002 Rule &amp; Supplemental Guidance (Day 0)</td>
<td>• Publish CUI Training (Day 180)</td>
<td>• Oversee Executive Branch Implementation</td>
<td>• Oversee Executive Branch Implementation</td>
</tr>
<tr>
<td>• Augment Registry</td>
<td>• Provide Additional Guidance as needed</td>
<td>• Resolve Disputes &amp; Complaints</td>
<td>• Collect Reporting Data</td>
</tr>
<tr>
<td>• Provide Awareness Materials &amp; Products</td>
<td>• Establish Schedule for On-site Reviews</td>
<td>• Initiate On-site Reviews</td>
<td>• Publish CUI Training (Day 180)</td>
</tr>
<tr>
<td>• Consult with OMB &amp; Provide Budget Guidance</td>
<td>• Provide Training Support &amp; Consultation</td>
<td></td>
<td>• Provide Additional Guidance as needed</td>
</tr>
<tr>
<td>• Review Agency Policies</td>
<td></td>
<td></td>
<td>• Establish Schedule for On-site Reviews</td>
</tr>
</tbody>
</table>

### Key D/A Activities

<table>
<thead>
<tr>
<th>Planning</th>
<th>Readiness</th>
<th>Initiation</th>
<th>Final</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assert Physical Safeguarding*</td>
<td>Conduct Training*</td>
<td>Initiate CUI Implementation</td>
<td>Eliminate Old Markings</td>
</tr>
<tr>
<td>Develop &amp; Publish Policy*</td>
<td>Develop Training/Awareness</td>
<td>Handle</td>
<td>Assure use of only New Markings</td>
</tr>
<tr>
<td>Develop Training/Awareness</td>
<td>Develop IT Transition Plan</td>
<td>Recognize</td>
<td>Complete IT Transition</td>
</tr>
<tr>
<td>Develop IT Transition Plan</td>
<td>Continue Internal Budget Planning</td>
<td>Receive</td>
<td>Meet Refresher Training Requirements</td>
</tr>
<tr>
<td>Continue Internal Budget Planning</td>
<td>Develop Self-Inspection Plan</td>
<td>Initiate IT Transition</td>
<td></td>
</tr>
<tr>
<td>Develop Self-Inspection Plan</td>
<td>Develop Process to Manage CUI Status Challenges</td>
<td>Permit Creation of CUI</td>
<td></td>
</tr>
<tr>
<td>Develop Process to Manage CUI Status Challenges</td>
<td></td>
<td>Initiate Self-Inspection Program</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Required for IOC

As of 3/17/15

**IOC**

**FOC**
What is needed to implement a CUI Program?

E.O. 13556 Sec. 5. Implementation (b):
After a review of agency plans, and in consultation with affected agencies and the Office of Management and Budget, the Executive Agent shall establish deadlines for phased implementation by agencies.

180 Days
- Policy
  - Roles and Responsibilities
  - Identify CUI handled
  - Specialized implementation

Year 1
- Suitable physical environment
- Training (of all affected personnel)
  - Basic
  - Specified
  - Implementers
  - Program Leads

Year 3-4
- Suitable electronic environment
  - Moderate Confidentiality
“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.
“In accordance with FIPS Publication 199, CUI Basic is categorized at the moderate confidentiality impact level. Agencies must also apply the appropriate requirements and controls from FIPS Publication 200 and NIST SP 800-53 to CUI consistently with any risk-based tailoring decisions that they make.” (proposed CUI regulation).
ISOO collaborated with NIST and DoD on developing NIST Special Publication 800-171, “Protecting Controlled Unclassified Information (CUI) in Non-Federal Systems and Organizations,” June 2015, to represent the technical standards and guidelines for Moderate Confidentiality in the contractor environment.
• 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 followed 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.
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.

The Department of Defense revised its DFARS to reference the new publication.
FAR Approach

Goal – the development of a FAR rule to protect CUI in the contractor community, by its reference to:

- EO 13556
- CUI EA issuances
- Agency CUI implementation policies (e.g., identifying the CUI categories and subcategories to be handled)
- NIST SP 800-171
- Include reporting of security incidents involving compromise
FAR Approach – Additional Points

- Additional Features
  - Completion of representations and certifications relevant to CUI in the System for Award Management (SAM) database
  - Requirement to keep current based on any changed status pertaining to CUI representations (e.g., safeguarding capabilities)
  - Future use of SAM database for oversight activities being explored with GSA for possible inclusion in FAR rule
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 process for incorporation in CFR

National Implementation Plan (NIP)
- Work with agencies and OMB to create and execute implementation planning framework, including deadlines for phased implementation

CUI Marking Handbook
Contact Information

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

(202) 357-5250 (voice)
(202) 357-5907 (fax)
isoo@nara.gov
cui@nara.gov

www.archives.gov/isoo or www.archives.gov/cui
The following slide is included for reference.
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