Controlled Unclassified Information

Shared • Standardized • Transparent

Information Security Oversight Office (ISOO)
Outline

- Why protect CUI?
  - Impacts to National Security

- Current Practices
  - CUI Program & Existing Agency Practices

- Information Security Reform
  - CUI Registry
  - 32CFR2002
  - NIST SP 800-171 (Rev 1)
  - Federal Acquisition Regulation

- Implementation
  - Leveraging Existing Resources
  - Costs and Budget for FY18
  - Implementation Reporting

- Understanding the CUI Program
Why protect CUI?

- The loss or improper safeguarding of CUI could be expected to have a **serious adverse effect** on organizational operations, organizational assets, or individuals.
  - 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;
  - significant damage to organizational assets;
  - significant financial loss; or
  - significant harm to individuals that does not involve loss of life or serious life threatening injuries

- The loss or improper safeguarding of CUI has a direct impact on national security
The OPM Data breach is a significant CUI incident
- Personnel files of 4.2 million former and current government employees.
- Security clearance background investigation information on 21.5 million individuals.

OPM failed to implement a longstanding requirement to use multi-factor authentication for network access.

“The intelligence and counterintelligence value of the stolen background investigation information for a foreign nation cannot be overstated, nor will it ever be fully known.”

September 7, 2016.

Government expense (to notify and protect those impacted) = $350 Million
Executive departments and agencies apply their own **ad-hoc policies** and markings to unclassified information that requires safeguarding or dissemination controls, resulting in:

- **Inefficient patchwork system** with more than 100 different policies and markings across the executive branch
- **Inconsistent** marking and safeguarding of documents
- **Unnecessarily restrictive** dissemination policies
- **Impediments** to authorized information sharing
The CUI Program is based on existing information safeguarding practices
   - Built in consultation with affected agencies (Data calls, CUI Advisory Council, working groups, etc)

Agencies are currently protecting “sensitive information”

CUI Program is a refinement and standardization of:
   - What the Executive branch protects; and
   - How information is protected.
Information Security Reform

- Clarifies and limits what to protect
- Defines safeguarding
- Promotes authorized information sharing
- Reinforces existing legislation and regulations
The CUI Registry is the repository for all information, guidance, policy, and requirements on handling CUI.

The CUI Registry is a catalogue of what the Executive branch should be protecting.

The CUI Registry identifies all approved CUI categories and subcategories, provides general descriptions for each, identifies the basis for controls, establishes markings, and includes guidance on handling procedures.

- Categories and Subcategories
- Limited Dissemination Controls
- Marking Guidance
- CUI Notices
- Training and awareness
- Annual Reports to the President
32 CFR 2002

- Implements the CUI Program
  - Establishes policy for designating, handling, and decontrolling information that qualifies as CUI
    - Effective: November 14, 2016
- 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
To promote standardization, the CUI Executive Agent plans to sponsor a Federal Acquisition Regulation (FAR) clause that uniformly apply the requirements contained in the 32 CFR Part 2002 and NIST SP 800-171 to industry.
Oversight to Industry

- System for Award Management
- Three tiers: Agency risk management decision based on CUI type, quantity, and purpose
  - Certification
  - Documentation
  - Validation

https://www.sam.gov
Implementation

- CUI Notice 2016-01, Implementation Guidance for the Controlled Unclassified Information Program
  - Allows for flexibility in meeting established milestones.

- Implementation activities began on November 14, 2016 (effective date of 32 CFR 2002)

- Implementation includes:
  - Program Management
  - Policy
  - Training
  - Physical Safeguarding
  - Incidents
  - Systems
  - Self Inspection
  - Contracts and agreements

Executive Branch
Implementation = 3-5 years
Leveraging Existing Resources

- Most agencies have existing SBU policies, training, and programs

- Agencies should leverage existing resources throughout implementation
  - Reallocate existing resources (personnel, funding, and time) to focus on CUI Implementation

- Implementation activities in FY17 are administrative in nature. Existing resources can be used to:
  - Identify and modify policy
  - Develop training
  - Assess systems
OMB A-11 Circular (July 2016), Section 31.15, requires that agency budget estimates consider the implementation of the CUI Program.

Agency estimates should reflect:

- Development of internal policies to phase-in and transition to the CUI program;
- Development and implementation of training programs to inform affected employees of their responsibilities when handling CUI;
- Assessment and any transition of information systems which handle or are used to process CUI;
- Implementation of physical safeguarding as required for CUI; and
- Development of an internal agency CUI self-inspection program.
Implementation Reporting

- ISO0, as the CUI Executive Agent, will monitor agency implementation actions
  - Agencies must assert and demonstrate implementation progress
- Agencies must report annually to ISO0
  - November 1st
  - Agencies convey projected implementation dates based on established implementation plans
Understanding the CUI Program

- CUI Basic versus CUI Specified
- Limitations of Agency Policy
- Controlled Environments
- Systems Requirements: Moderate
  - NIST SP 800-171 (Rev 1)
- 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)
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.
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 (//).
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.
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.
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.
Destruction

- Unreadable, Indecipherable, and Irrecoverable
- NIST SP 800-88, Guidelines for Media Sanitization

Destroy paper using cross cut shredders that produce particles that are 1mm by 5 mm.
Questions?