Controlled Unclassified Information

Unauthorized Disclosures: Prevention and Reporting

Shared • Standardized • Transparent

ISOO
INFORMATION SECURITY
OVERSIGHT OFFICE

Information Security Oversight Office (ISOO)

Outline

- What is Controlled Unclassified Information?
- Why protect CUI?
- Impacts to National Security
- Leaks, Espionage, and Spills
- Safeguarding Measures
- The Insider Threat
- Reporting

What is Controlled Unclassified Information or CUI?

- CUI is information that needs protection. Laws, Regulations, or Government wide policies call for this information to be protected.
  - The **CUI Registry** provides information on the specific categories and subcategories of information that the Executive branch protects. The CUI Registry can be found at: https://www.archives.gov/cui

- CUI includes, but is not limited to:
  - Privacy (including Health)
  - Tax
  - Law Enforcement
  - Critical Infrastructure
  - Export Control
  - Financial
  - Intelligence
  - Privilege
  - Unclassified Nuclear
  - Procurement and Acquisition

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

Impacts to 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.

"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."

– *The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation*
September 7, 2016.

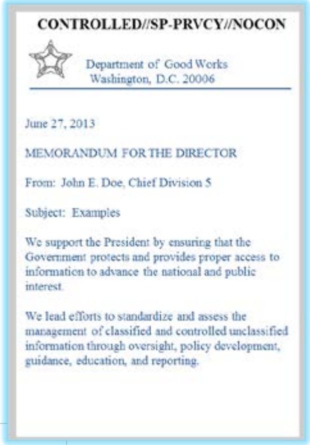
Government expense (to notify and protect those impacted) = $350 Million

Leaks, Espionage, and Spills

- **Leaks** – When CUI is deliberately disclosed (media).
- **Espionage** – Activities designed to obtain or transmit CUI in order to harm the United States or to provide advantage to a foreign nation or transnational entity.
- **Spill** – The willful, negligent, or inadvertent disclosure of CUI across computer systems (internet and email).

Safeguarding measures

- Policy and procedures
- Training and awareness
- Physical and Electronic protections
- Oversight Measures
- Reporting



CONTROLLED//SP-PRVCY//NOCON

Department of Good Works
Washington, D.C. 20006

June 27, 2013

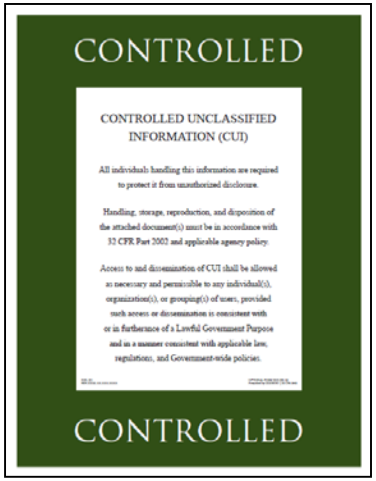
MEMORANDUM FOR THE DIRECTOR

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.



CONTROLLED

CONTROLLED UNCLASSIFIED INFORMATION (CUI)

All individuals handling this information are required to protect it from unauthorized disclosure.

Handling, storage, reproduction, and disposition of the attached document(s) must be in accordance with 32 CFR Part 2002 and applicable agency policy.

Access to and dissemination of CUI shall be allowed as necessary and permissible to any individual(s), organization(s), or grouping(s) of users, provided such access or dissemination is consistent with or in furtherance of a Lawful Government Purpose and in a manner consistent with applicable law, regulations, and Government-wide policies.

CONTROLLED

CUI Registry = What we protect

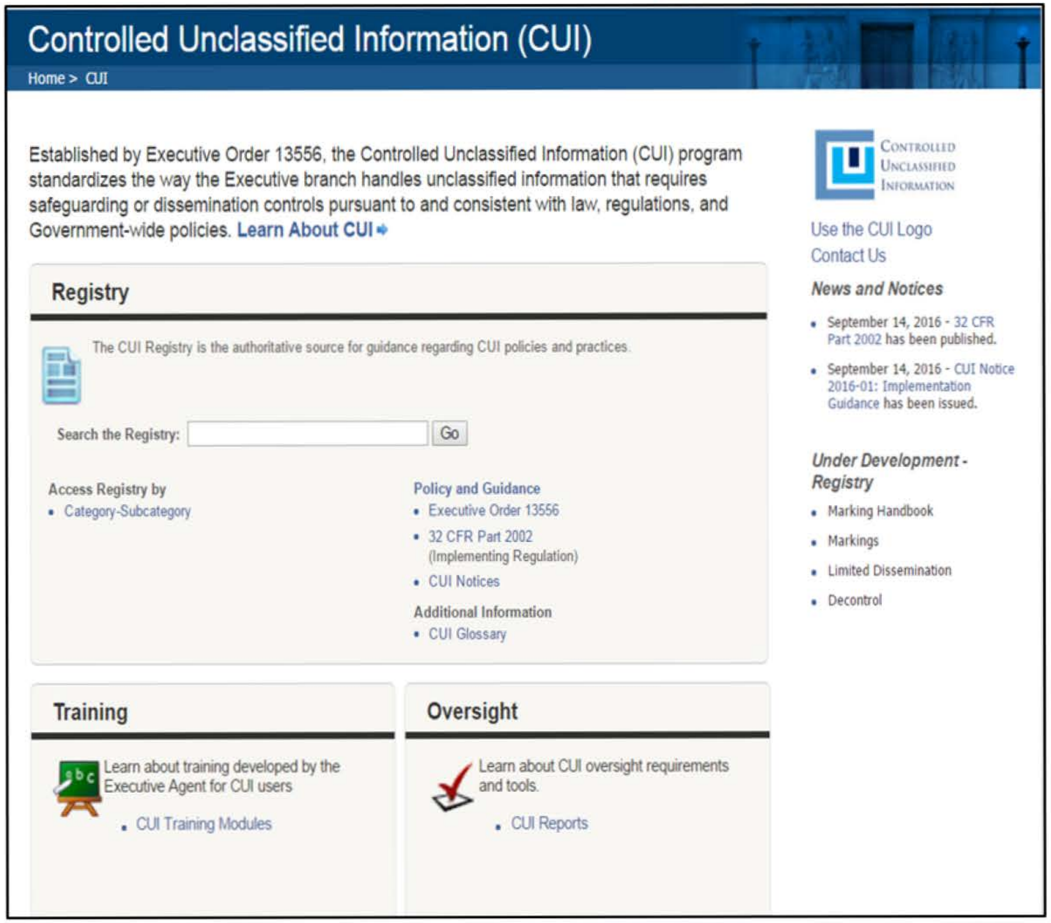
The CUI Registry is the repository for all information, guidance, policy, and requirements on handling CUI.

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

www.archives.gov/cui



Controlled Unclassified Information (CUI)

Home > CUI

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
- 32 CFR Part 2002 (Implementing Regulation)
- 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

Use the CUI Logo

Contact Us

News and Notices
- September 14, 2016 - 32 CFR Part 2002 has been published.
- September 14, 2016 - CUI Notice 2016-01: Implementation Guidance has been issued.

Under Development - Registry
- Marking Handbook
- Markings
- Limited Dissemination
- Decontrol

General Safeguarding Policy

- 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.

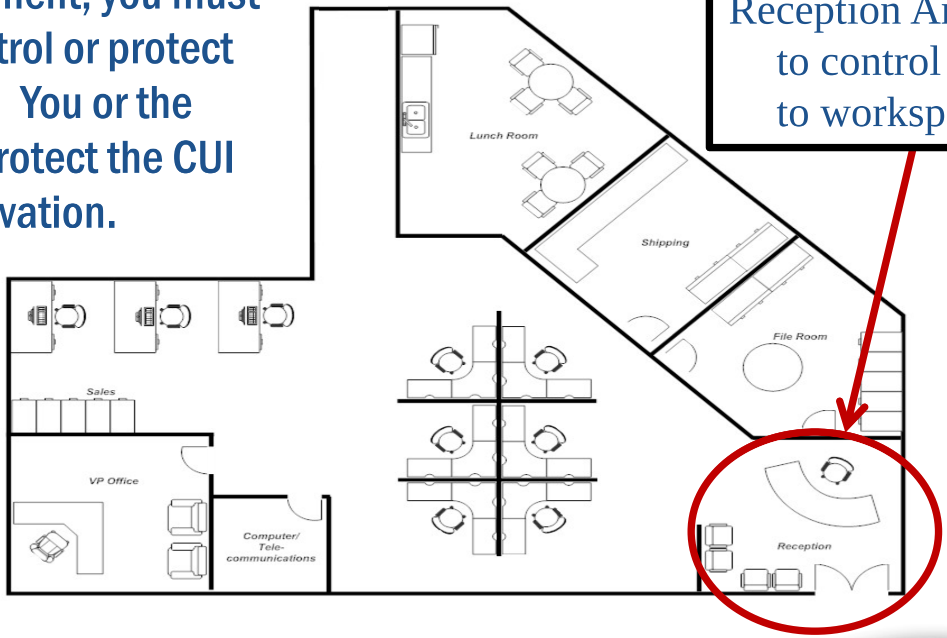
- Safeguarding measures that are authorized or accredited for classified information are sufficient for safeguarding CUI.

- Follow agency policy and procedure.

Controlled Environments (physical)

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.



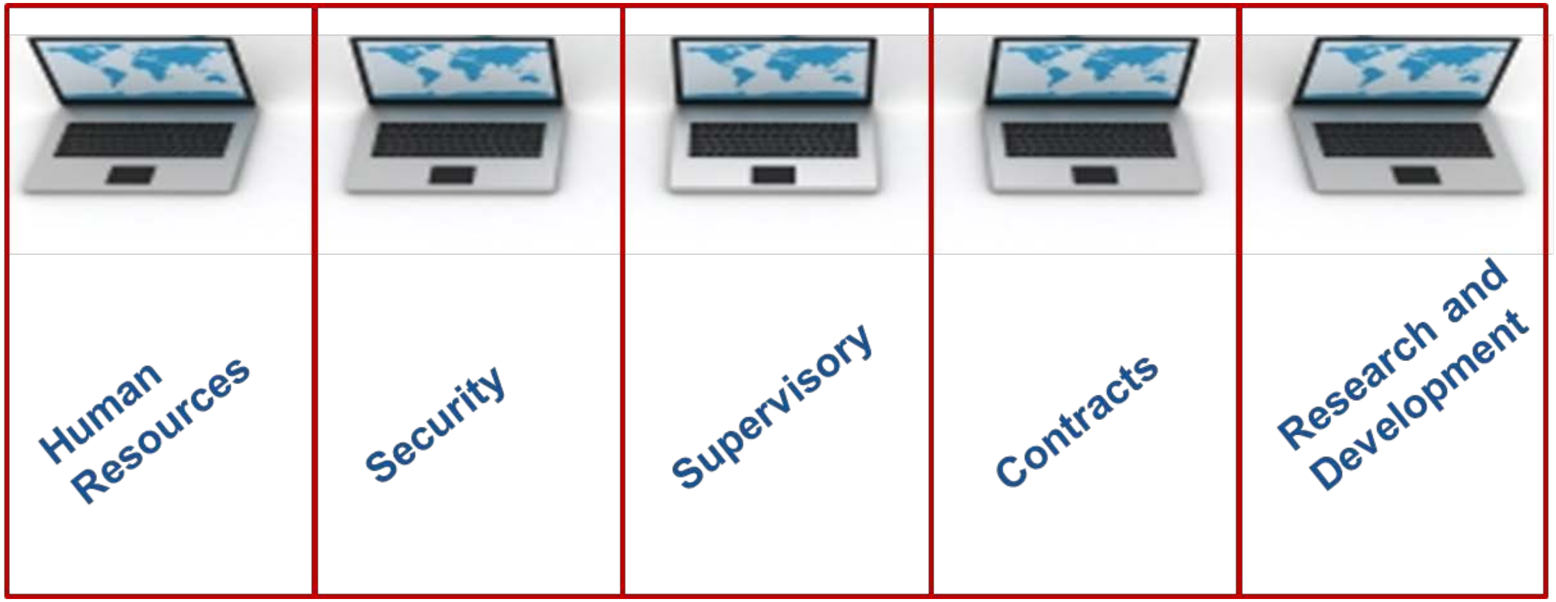
Reception Area used to control access to workspace.

Controlled Environments (Electronic)

Limit and control access to CUI within the workforce by establishing electronic barriers.

- Dedicated network drives, SharePoint sites, intranet sites

- Assess who has a lawful government purpose for access



Human Resources

Security

Supervisory

Contracts

Research and Development

The Insider Threat

- Any person with authorized access to any government resource to include personnel, facilities, information, equipment, networks or systems.
- Indicators:
  - General disregard for security procedures
  - Seeking access to information outside the scope of current responsibilities
  - Attempting to enter or access to sensitive areas (where CUI is stored, discussed, or processed)
  - Inconsistent working hours (staying late or arriving early)
  - Unusual insistence on working in private
  - Depressed or disgruntled

Reporting

- Employees are required to report:
  - Any actual or suspected mishandling of CUI
  - Any suspicious behaviors among the workforce that could potentially compromise or lead to the misuse of CUI
- Report to your security manager or officer.
- **When in doubt, report it!**

Summary

- Review any applicable agency/organizational policy
- Familiarize yourself with what to protect and how to protect it.
- Be on the lookout for suspicious behavior among the workforce
- Know how to report to security