Controlled Unclassified Information

The Program, Implementation, and Features

Shared • Standardized • Transparent

ISOO
INFORMATION SECURITY OVERSIGHT OFFICE

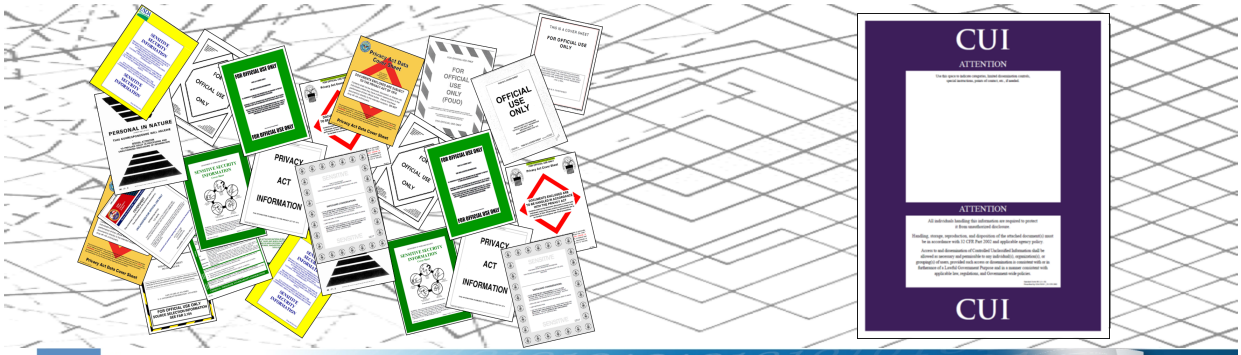
Information Security Oversight Office (ISOO)

Outline

- An Information Security Reform
- What is CUI
- The CUI Registry
- CUI in Contracts and Agreements
- Cyber Security Requirements

Information Security Reform

- Clarifies what to protect
- Defines safeguarding
- Reinforces existing LRGWP
- Promotes authorized information sharing



What is Controlled Unclassified Information (CUI)?

- **CUI is information that needs protection.** Laws, Regulations, or Government wide policies call for this information to be protected.

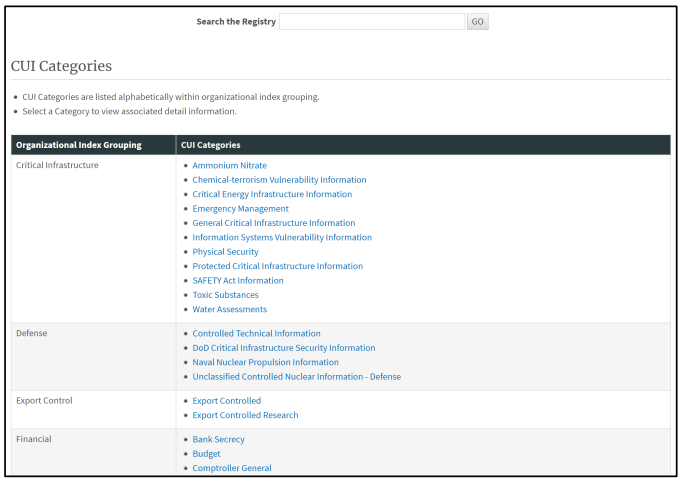
  - The **CUI Registry** provides information on the specific categories of information that the Executive branch protects. The CUI Registry can be found at:

The CUI Registry

Online Searchable Living

Contains:

- Categories
- Descriptions
- Markings
- Links to Policy



Search the Registry GO

CUI Categories

- CUI Categories are listed alphabetically within organizational index grouping.
- Select a Category to view associated detail information.

Organizational Index Grouping	CUI Categories
Critical Infrastructure	• Ammonium Nitrate • Chemical-terrorism Vulnerability Information • Critical Energy Infrastructure Information • Emergency Management • General Critical Infrastructure Information • Information Systems Vulnerability Information • Physical Security • Protected Critical Infrastructure Information • SAFETY Act Information • Toxic Substances • Water Assessments
Defense	• Controlled Technical Information • DoD Critical Infrastructure Security Information • Naval Nuclear Propulsion Information • Unclassified Controlled Nuclear Information - Defense
Export Control	• Export Controlled • Export Controlled Research
Financial	• Bank Secrecy • Budget • Comptroller General

CUI Basic and CUI Specified

CUI Specified
(Requires unique markings)

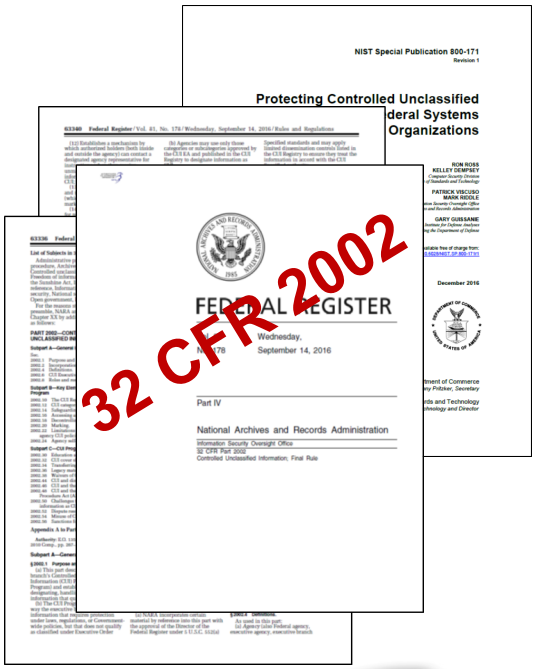
Laws, Regulations, or Government-wide policies require specific protections. For example:

- Unique markings
- Enhanced physical safeguards
- Limits on who can access the information

CUI Basic

Laws, Regulations, or Government-wide policies **DO NOT** require specific protections.

What we protect and How we protect it



Implementation

- Implementation has begun
  - Program officials, resources, policy, training, systems, contracts, oversight
- **CUI practices and Legacy practices will exist at the same time.**

Federal Acquisition Regulation (FY19)

"This FAR rule is necessary to ensure uniform implementation of the requirements of the CUI program in contracts across the government, thereby avoiding potentially inconsistent agency-level action." –Unified Agenda

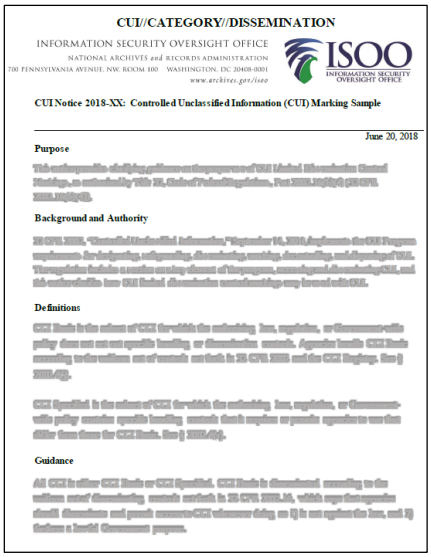
The FAR is still going through the process of review and approval prior to public comment.

a) When the FAR is released for public comment we will have a blog post about when/how to comment.

b) We will also announce an ad hoc stakeholders meeting to address questions about the proposed FAR changes (this will be limited to answering questions about the content of the proposed FAR changes and will not accept or adjudicate any changes).

Marking CUI

- Purpose is to inform or alert recipients/users that CUI is present and of any limited dissemination controls.
- Agencies must uniformly and conspicuously apply CUI markings to all CUI prior to disseminating it.
- The CUI banner marking must appear, at a minimum, at the top center of each page containing CUI.



CUI//CATEGORY//DISSEMINATION

INFORMATION SECURITY OVERSIGHT OFFICE
NATIONAL ARCHIVES and RECORDS ADMINISTRATION
700 PENNSYLVANIA AVENUE, NW ROOM 100 WASHINGTON, DC 20408-0001
www.archives.gov/isoo

ISOO INFORMATION SECURITY OVERSIGHT OFFICE

CUI Notice 2018-XX: Controlled Unclassified Information (CUI) Marking Sample

June 20, 2018

Purpose

Background and Authority

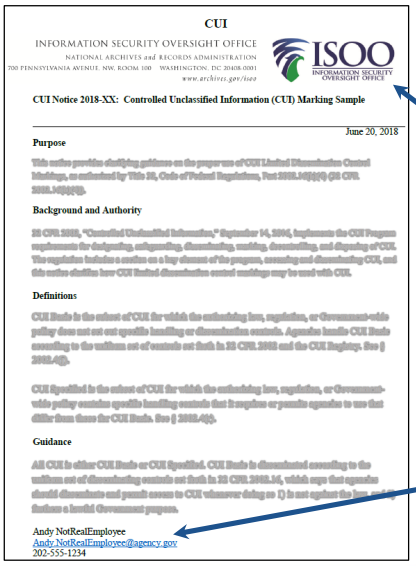
Definitions

Guidance

Designation Indicator

Designation Indicators show which agency made the document CUI and are mandatory

- It is best practice to include **contact information**


CUI

INFORMATION SECURITY OVERSIGHT OFFICE
NATIONAL ARCHIVES and RECORDS ADMINISTRATION
700 PENNSYLVANIA AVENUE, NW, ROOM 100 WASHINGTON, DC 20408-0001
www.archives.gov/isoo

CUI Notice 2018-XX: Controlled Unclassified Information (CUI) Marking Sample

June 20, 2018

Purpose

Background and Authority

Definitions

Guidance

Andy NotRealEmployee
Andy.NotRealEmployee@agency.gov
202-555-1234

Mandatory Designating Agency Indicator

Optional Contact Information

Three Elements of the Banner Marking

- The CUI Control Marking (mandatory) may consist of either "CONTROLLED" or "CUI."
- CUI Category Markings (mandatory for CUI Specified). CUI Control Markings and Category Markings are separated by two forward slashes (//). When including multiple categories they are separated by a single forward slash (/).
- Limited Dissemination Control Markings. Limited Dissemination Control Markings are separated from the rest of the Banner Marking by a double forward slash (//).

CUI Banner Marking

CUI//CATEGORY//DISSEMINATION

INFORMATION SECURITY OVERSIGHT OFFICE
NATIONAL ARCHIVES and RECORDS ADMINISTRATION
700 PENNSYLVANIA AVENUE, NW, ROOM 100 WASHINGTON, DC 20408-0001
www.archives.gov/isoo

CUI Notice 2018-XX: Controlled Unclassified Information (CUI) Marking Sample

June 20, 2018

Purpose

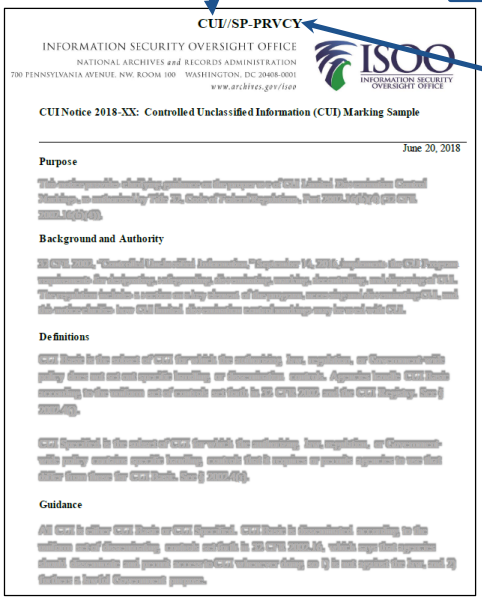
Background and Authority

Definitions

Guidance

CUI Specified Category Marking

- The CUI Category Marking is **mandatory** for CUI Specified
- The general form for CUI Specified Category Marking is **SP-SPECIFIED**



CUI Registry:
https://www.archives.gov/cui/registry/category-marking-list

CUI and Metadata

The CUI advisory council created an interoperability working group dedicated to advancing standardization/interoperability of non-human readable CUI markings.

The working group has partnered with NIEM

The National Information Exchange Model (NIEM) is a common vocabulary that enables efficient information exchange across diverse public and private organizations. NIEM connects communities of people who share a common need to exchange information in order to advance their mission. https://www.niem.gov/about-niem

NIST SP 800-171

Current:

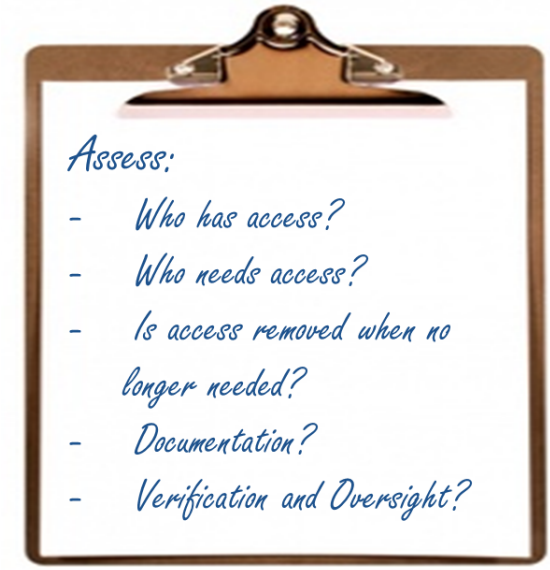
- NIST SP 800-171 Rev 1
- NIST SP 800-171A
- SSP Template (optional)
- Plan of Action Template (optional)
- Mapping from Cyber Security Framework v1.0 to 171
- NIST MEP Handbook

Planned:

- NIST SP 800-171 Rev 2
- NIST SP 800-171b
- NIST SP 800-53 Rev 5 (Currently in review at the Office of Management and Budget Office of Information and Regulatory Affairs.)

Assessing electronic Environments

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



Other Considerations

- Personal Devices
- Telework
- Bring/Use your own device
- USB Drives
- Travel
- Separation and transfers
- Insider Threats

Upcoming Events

INDUSTRY DAY

February 11, 2020

From 10:00 to 2:00 pm

CUI Stakeholder Meeting

February 12, 2020

From 1:00 to 3:00 pm.

Learn more about CUI

Website

www.archives.gov/cui

Blog

https://isoo.blogs.archives.gov/

Email

CUI@NARA.GOV

Questions?