Information Security Oversight Office

Protect • Inform • Assess

NISP Update NDIA/AIA

John P. Fitzpatrick, Director

May 19, 2015

Agenda

- Cybersecurity Information Sharing and the NISP
- NISP Working Group Update
- CUI Program Update

Executive Order 13691

- "Promoting Private Sector Cybersecurity Information Sharing"
- Secretary of DHS has the lead
- "…encourage the development and formation of Information Sharing and Analysis Organizations (ISAOs)"
- "…common set of voluntary standards…[to] further the goal of creating robust information sharing related to cybersecurity risks and incidents
- "..standards shall address…contractual agreements, business processes, operating procedures, technical means, and privacy protections…"

Executive Order 13691

- Promote Sharing = Private sector to private sector, as well as with the government
- In some instances, with some ISAOs, DHS may seek to share classified national security information
- EO13681 amends EO 12829 “National Industrial Security Program”
- Names DHS as having responsibility for CIPP policy within the NISP
- DHS joins other CSAs DoD, DNI, DoE and NRC
- Facility clearances when storing/processing CNSI
- DHS hybrid for entities new to NISP

SAP Working Group Overview

- **Industry requested re-establishment of the SAP working group through NISPPAC to address industry issues/concerns which included:**
  - **Joint SAP Implementation Guide (JSIG) requirements.**
    - **Status on publication of the four DoD volumes**
    - **Timeframe for release to coincide with Conforming Change 2**
    - **Transition from JAFAN and NISPOM supplement to JSIG**
  - **Implementation of Risk Management Framework (RMF)**
  - **Two person integrity (TPI) and System access and approval process**
  - **Program Security Offices mandating requirements inconsistently across programs.**

- **ISOO held meetings with Agencies authorized to create SAPs and NISP Industry and Contractor Special Security Working Group (CSSWG) Reps**
  - **Concern over replacement for NISPOM SAP Supplement**
  - **Replaced by Appendix D of Conforming Change 2**

- **Meetings**
  - **Held on March 10,2014 and May, 5, 2015**
    - **With ISOO, SAP Agencies, and Industry**
    - **Next meeting week of July 6, 2015 at National Archives.**

Policy Integration Working Group

Established to enhance the integration between NISP guidance and other authoritative guidance in the government

- **NISPPAC Industry expressed concern over the "fracturing" of the NISP**

- **Establish a coordination process for policy impacting NISP industry and agencies**
  - Critical infrastructure programs
  - Cyber security
  - Controlled unclassified information
  - Insider threat programs

- **First meeting Jan 2015. Next meeting June 2015**

- **PIWG Representation includes NISP CSAs, CSOs & NISPPAC Reps**

CUI Approach for Contractor Environment

Government

E.O. 13556

Registry

32 CFR 2002

NIST SP 800-171

FAR

Industry

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.

Three-part Plan for CUI Protection

- Federal CUI rule (32 CFR Part 2002) to establish the required controls and markings for CUI governmentwide.
- NIST Special Publication 800-171 to define security requirements for protecting CUI in nonfederal information systems and organizations.
- Federal Acquisition Regulation (FAR) clause to apply the requirements of the federal CUI rule and NIST Special Publication 800-171 to contractors.

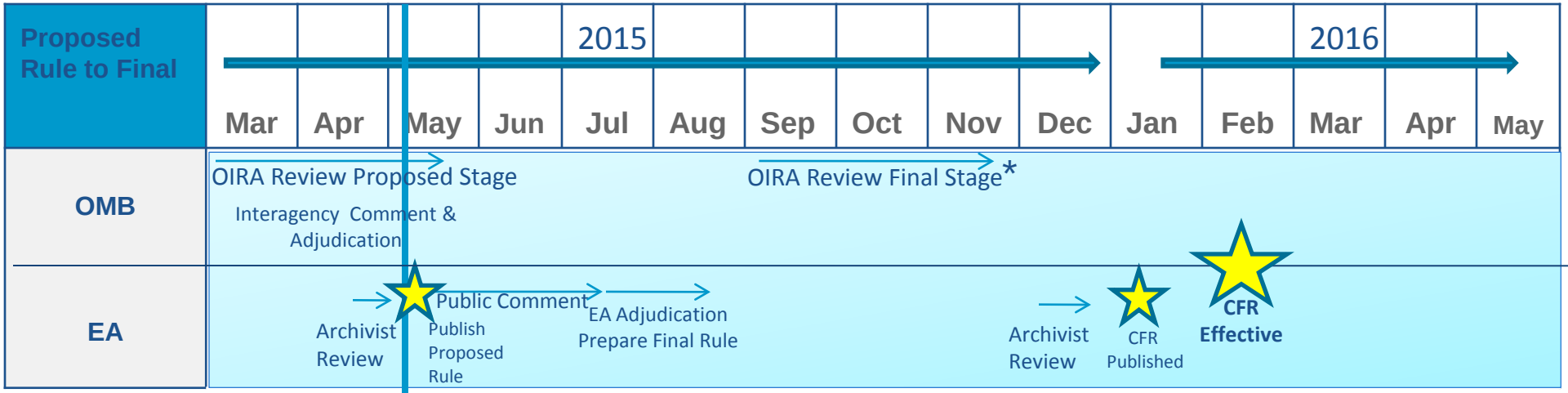
Draft CUI Regulation Out for Comment

- Proposed Rule 32 CFR 2002 Controlled Unclassified Information is in the Federal Register
- Comments Due 7 July
- Open Meeting 28 May 0930 hrs at National Archives on Pennsylvania Ave
- Offer: separate meeting with your group
- Link here: **http://tinyurl.com/ne5o5qd**

CUI Policy Status

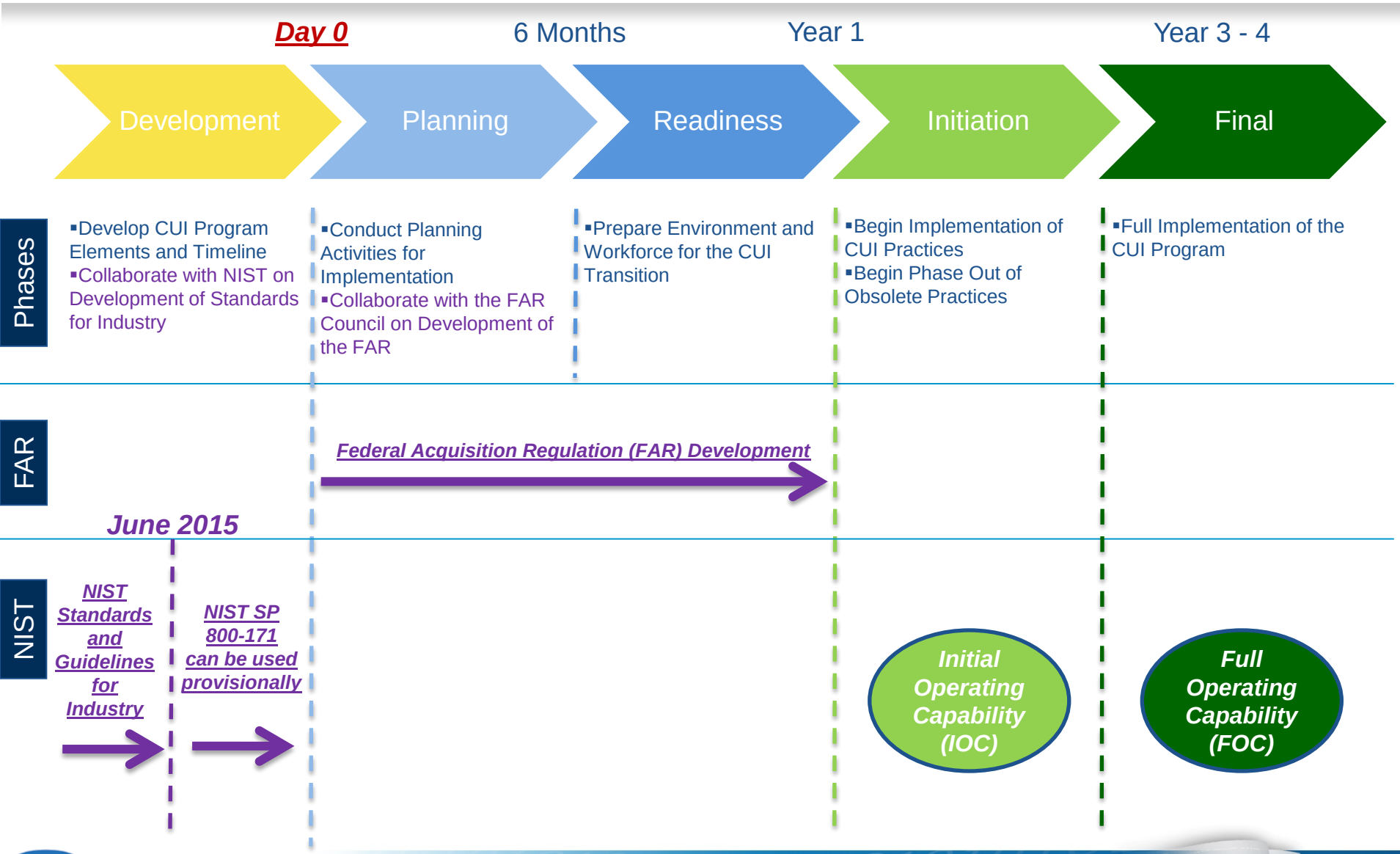
Projected CUI Policy Timeline

as of 5 May 2015



* Unlikely to require full 90 days

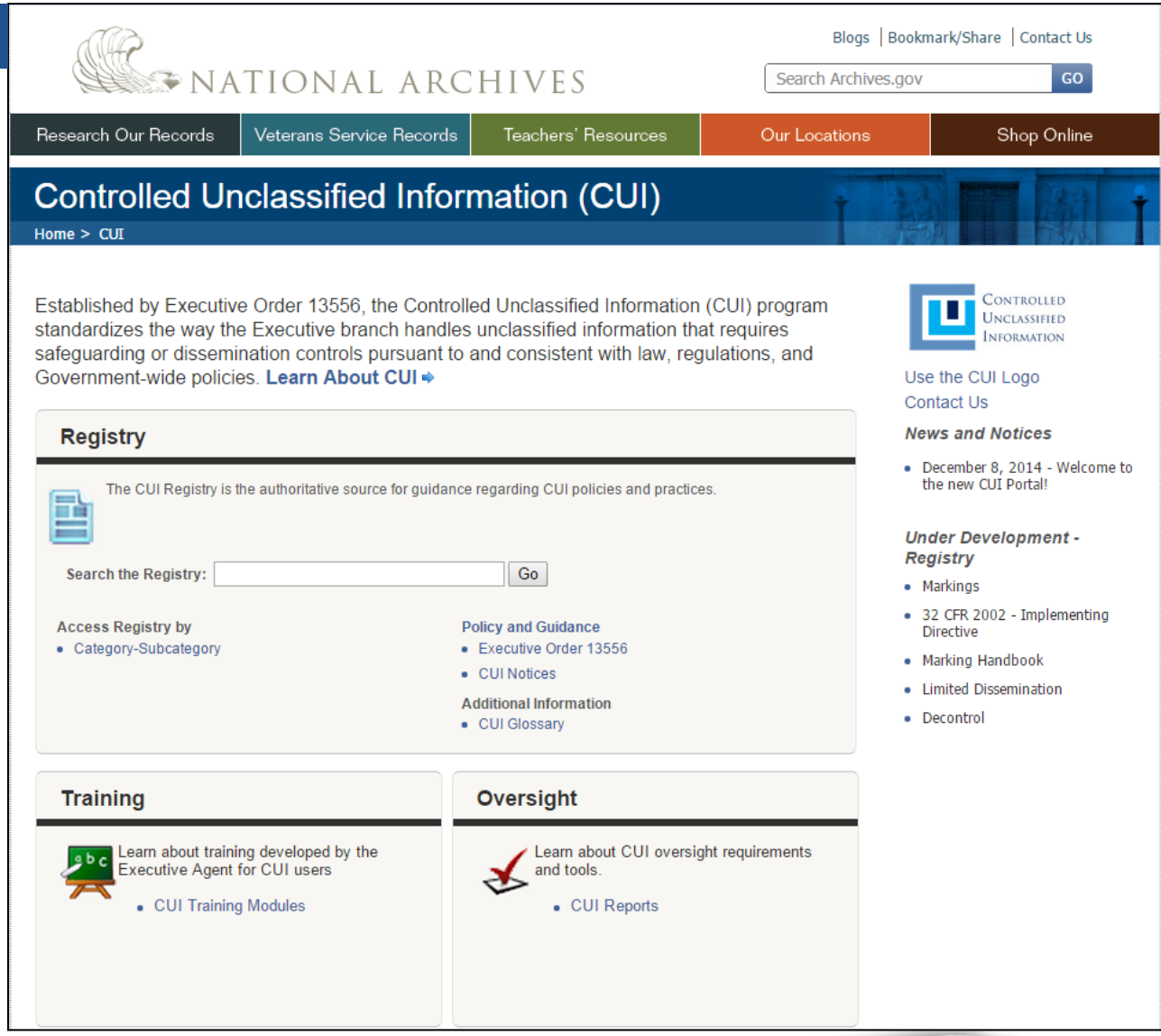
CUI Phased Implementation - FAR & NIST



Online Registry

http://www.archives.gov/cui

- 23 Categories
- 82 Sub-categories
- 315 unique Control citations
- 106 unique Sanction citations



Handling CUI

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

Two types: Basic and Specified

CUI Basic versus CUI Specified

- CUI Basic = LRGWP identifies an information type and says protect it.
- CUI Specified = LRGWP identifies an information type and says protect it but specifies exactly how to should be protected or handled.

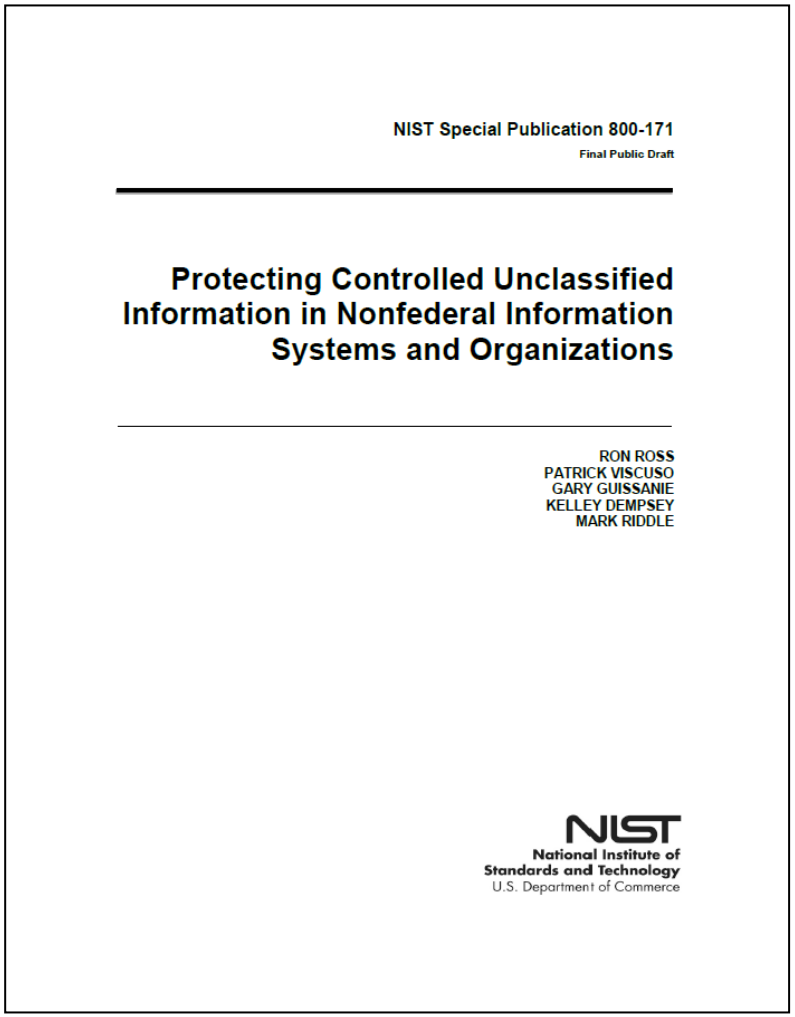
Contracts

Contractors handling CUI on behalf of an agency

- Executive branch agencies must include a requirement to comply with Executive Order 13556, Controlled Unclassified Information and 32 CFR Part 2002 in all contracts that require a contractor to handle CUI for the agency. The contractual requirement must be consistent with standards prescribed by the CUI Executive Agent.

DRAFT 32 CFR 2002

NIST Special Publication 800-171


NIST Special Publication 800-171
Final Public Draft

Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

RON ROSS
PATRICK VISCUSO
GARY GUISSANIE
KELLEY DEMPSEY
MARK RIDDLE

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Final Public Comment Period

Endsed May 12, 2015

The final publication of Special Publication 800-171 is targeted for June 2015

Purpose

- To provide federal agencies with recommended requirements for protecting the confidentiality of CUI —
  - ***When the CUI is resident in nonfederal information systems and organizations.***
  - ***Where the CUI does not have specific safeguarding requirements prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category or subcategory listed in the CUI Registry.***
  - ***When the information systems where the CUI resides are not operated by organizations on behalf of the federal government.***

Applicability

- CUI requirements apply only to components of nonfederal information systems that process, store, or transmit CUI, or provide security protection for such components.
  - ***The requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations.***

Definitions

- Federal Information System

An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

-- Federal Information Security Management Act (40 U.S.C., Sec. 11331)

- Nonfederal Information System

An information system that does not meet the criteria for a federal information system.

-- NIST Special Publication 800-171

- Nonfederal Organizations

An entity that owns, operates, or maintains a nonfederal information system (contractors, SLT, academia).

-- NIST Special Publication 800-171

Assumptions

- Statutory and regulatory requirements for the protection of CUI are *consistent*, whether such information resides in federal information systems or nonfederal information systems.
- Safeguards implemented to protect CUI are *consistent* in both federal and nonfederal information systems and organizations.
- CUI is categorized at the *moderate* confidentiality impact level in accordance with FIPS Publication 199.

Additional Assumptions

Nonfederal Organizations —

- Have information technology infrastructures in place.
  - Are not developing or acquiring systems specifically for the purpose of processing, storing, or transmitting CUI.
- Have safeguarding measures in place to protect their information.
  - May also be sufficient to satisfy the CUI requirements.
- May not have the necessary organizational structure or resources to satisfy every CUI security requirement.
  - Can implement alternative, but equally effective, security measures.
- Can implement a variety of potential security solutions.
  - Directly or through the use of managed services.

Security Control Requirements

- The basic security requirements are obtained from FIPS Publication 200, which provides the high-level and fundamental security requirements for federal information and information systems.
- The derived security requirements, which supplement the basic security requirements, are taken from the security controls in NIST Special Publication 800-53.
- The FIPS Publication 200 security requirements and the security controls in the *moderate baseline*, the requirements and controls are *tailored to eliminate requirements that are:*
- Allows for compensation measures to meet FIPS 200 targets

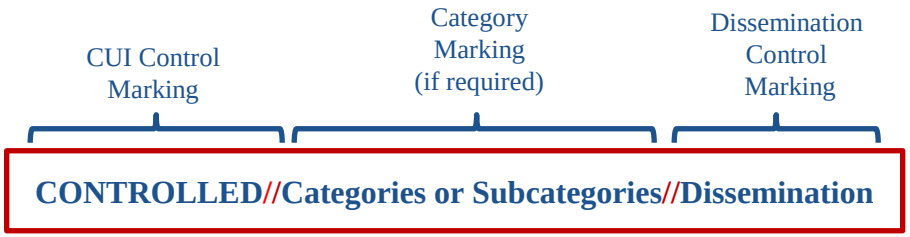
1. Uniquely federal (i.e., primarily the responsibility of the federal government);
2. Not directly related to protecting the confidentiality of CUI; or
3. Expected to be routinely satisfied by nonfederal organizations without specification.

Marking Handbook

DRAFT

Banner Marking

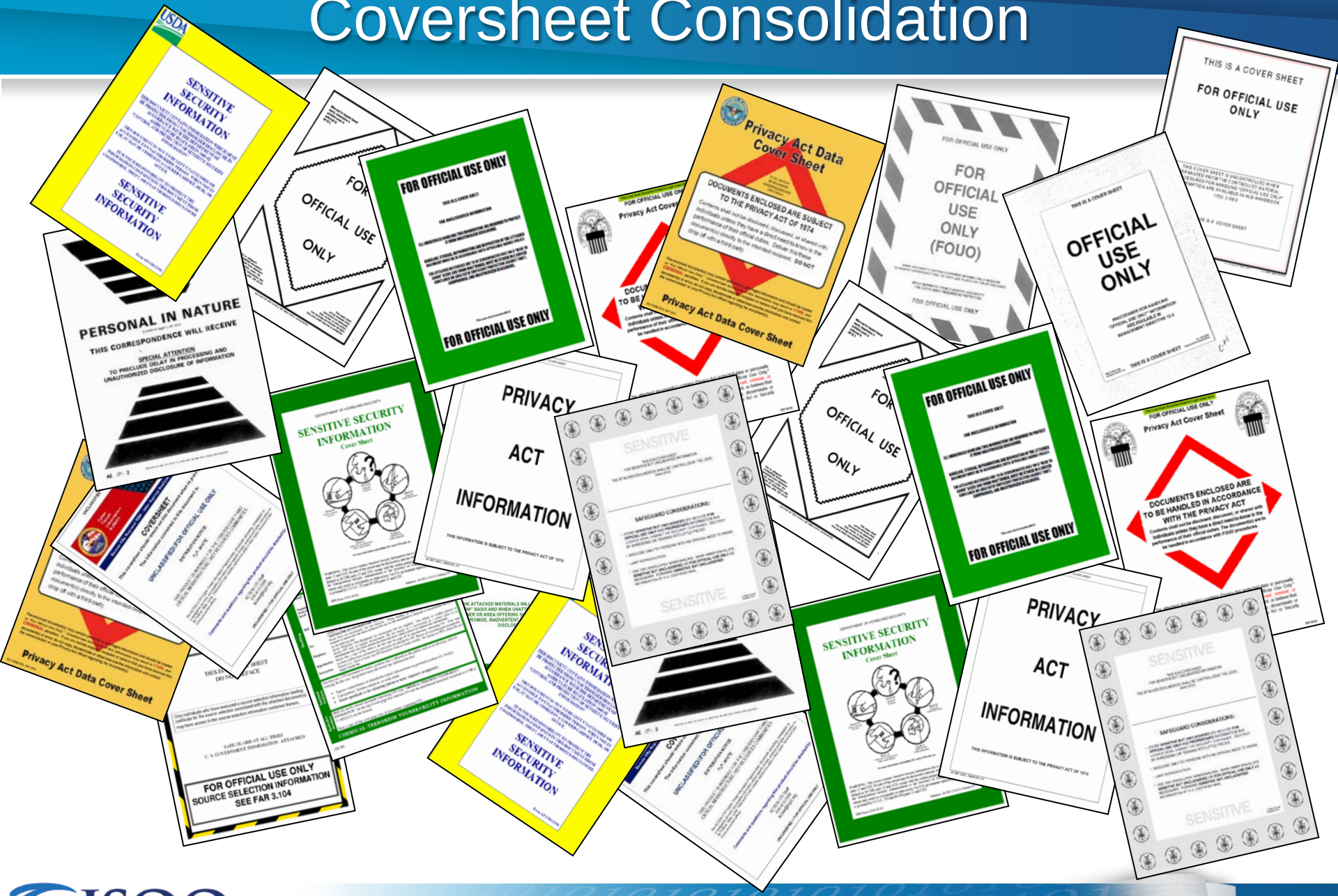
The banner marking consists of the CUI control marking, category markings (if required), and dissemination control markings.



Top center of each page containing CUI

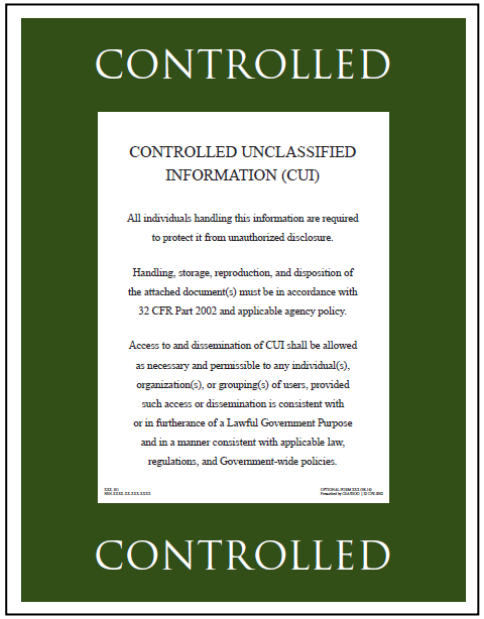
- The CUI control marking (the word "CONTROLLED" or the acronym "CUI") is mandatory for all CUI banners.
- Category markings are mandatory in the case of CUI Specified, and for CUI Basic when required by agency policy. Either complete category names or abbreviations may be used in banners to designate the categories of CUI contained within the document.
- All dissemination control markings must be approved by the CUI EA and published in the CUI Registry. Access to and dissemination of CUI must be allowed as extensively as necessary, consistent with or in furtherance of a Lawful Government Purpose.

Coversheet Consolidation

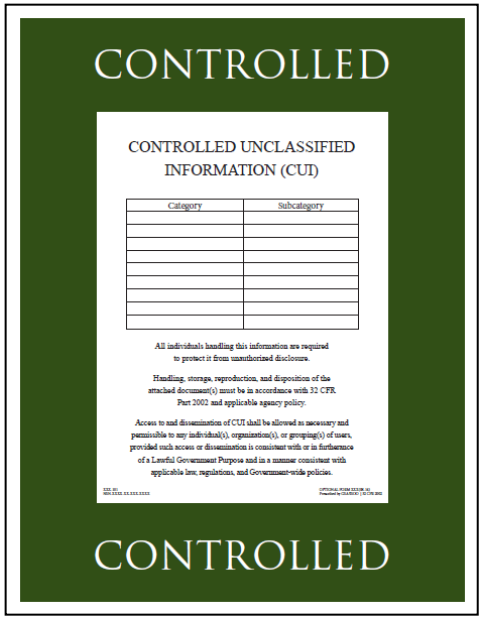


ISOO
INFORMATION SECURITY OVERSIGHT OFFICE

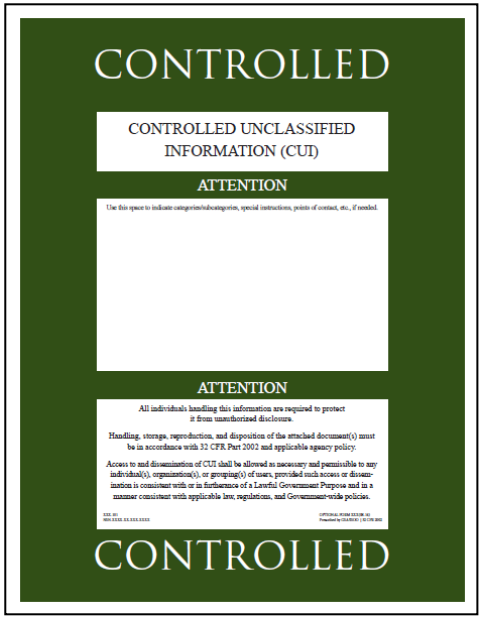
New Coversheets: Optional Forms



Optional Form 901. Basic CUI Coversheet. Acceptable for all forms of CUI.

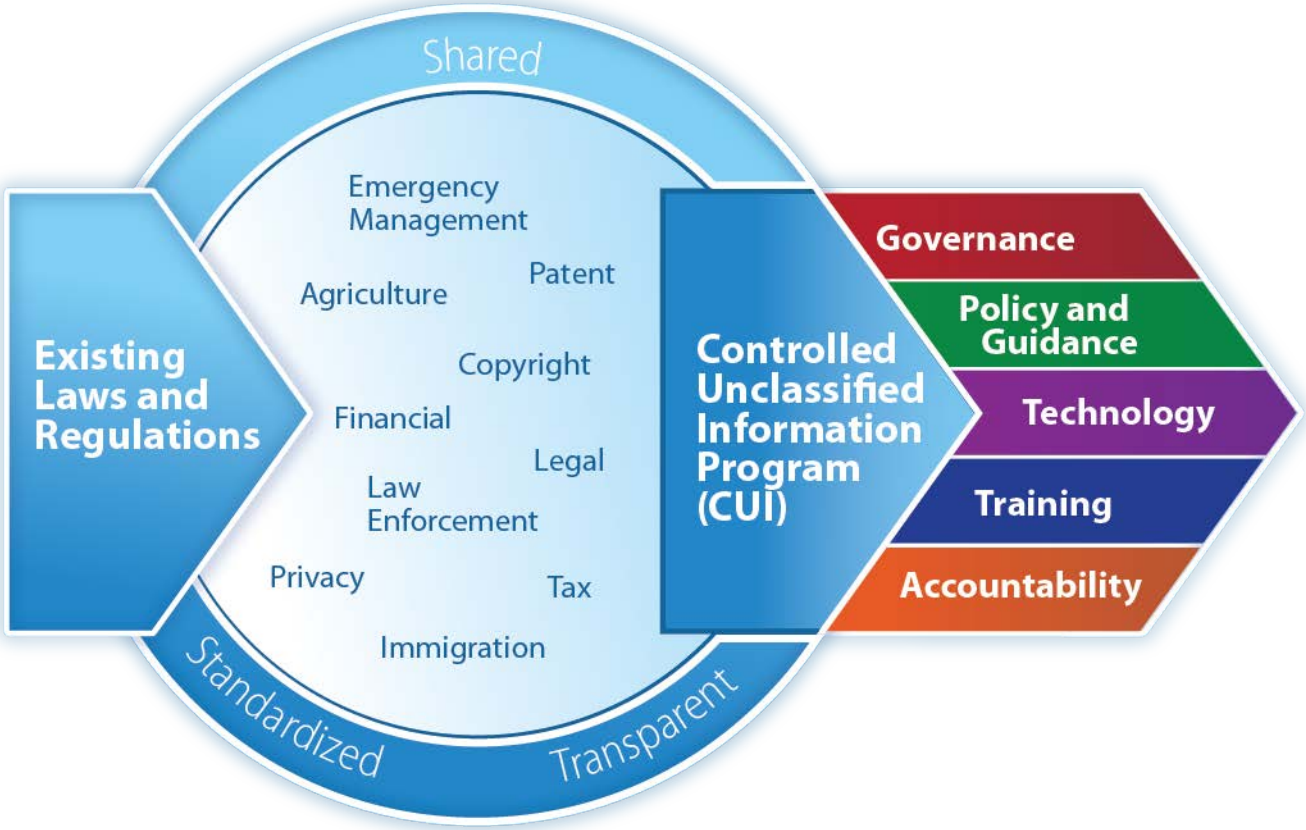


Optional Form 902. Category/Subcategory CUI Coversheet. Acceptable for all forms of CUI. Categories or Subcategories can be identified in the spaces provided.

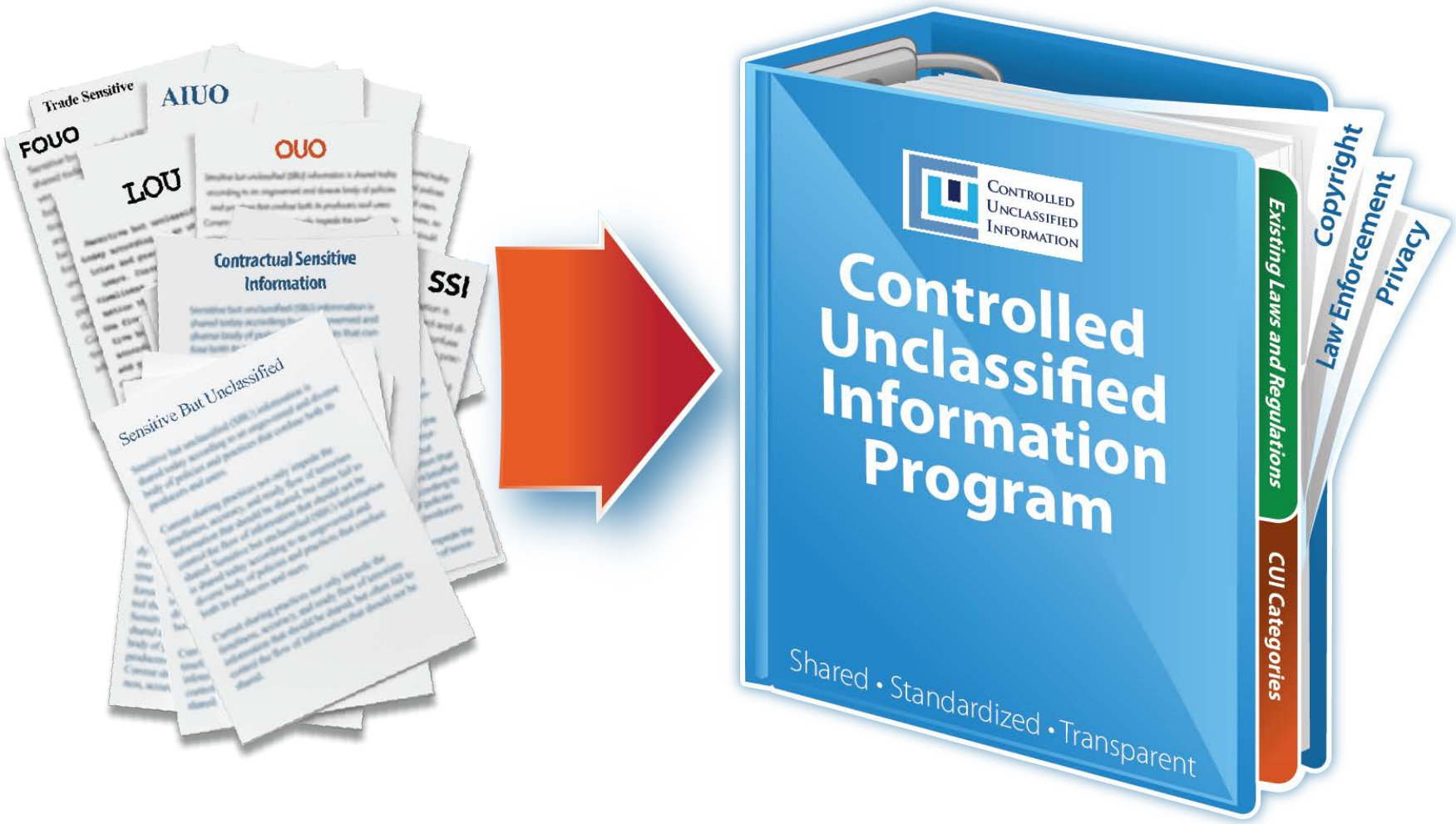


Optional Form 903. Detailed CUI Coversheet. Acceptable for all forms of CUI. The space indicated can be used to convey specific categories or subcategories used, special instructions, or relevant points of contact.

Questions?


Shared
Emergency Management
Patent
Agriculture
Copyright
Financial
Legal
Law Enforcement
Privacy
Tax
Immigration
Standardized
Transparent
Existing Laws and Regulations
Controlled Unclassified Information Program (CUI)
Governance
Policy and Guidance
Technology
Training
Accountability

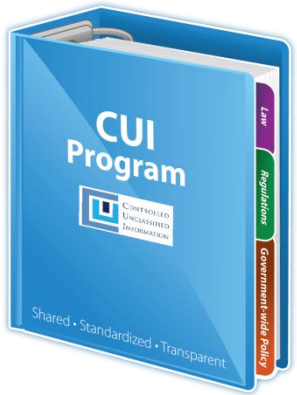
Overview of the CUI Program



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

23 Categories		82 Subcategories
Agriculture	Law Enforcement	• Bank Secrecy • DNA • Investigation
Controlled Technical Information	Legal	
Copyright	NATO	
Critical Infrastructure	Nuclear	
Export Control	Patent	
Emergency Management	Privacy	• Financial • Health Information • Personnel
Financial	Proprietary Business	
Foreign Government	Safety Act Information	
Geodetic Product Information	Statistical	• Census • Investment Survey
Immigration	Tax	
Information Systems Vulnerability Information	Transportation	
Intelligence		

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