Controlled Unclassified Information

Executive Order 13556

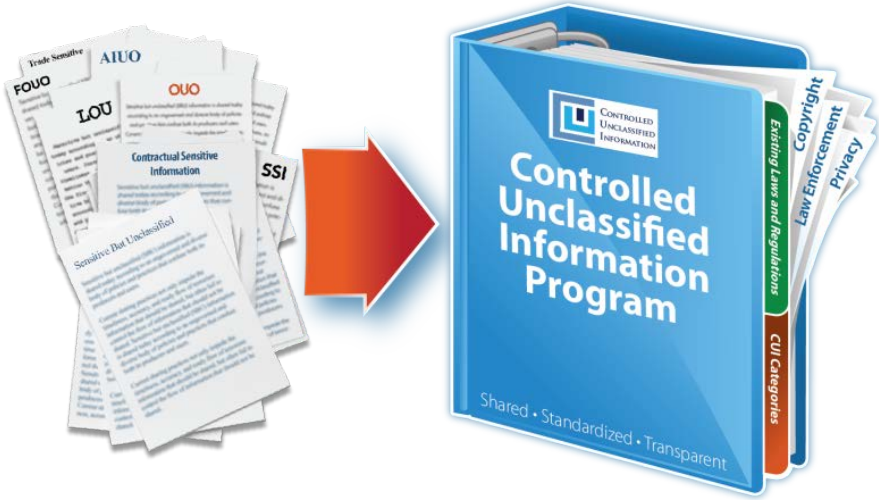
Shared • Standardized • Transparent

CONTROLLED
UNCLASSIFIED
INFORMATION

Information Security Oversight Office (ISOO)

Briefing Outline

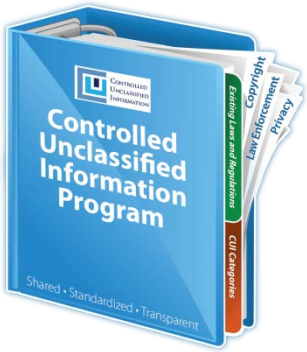
- Executive Order 13556
- CUI Registry
- 32 CFR, Part 2002
- Understanding the CUI Program
- Phased Implementation
- Approach to Contractor Environment



Executive Order 13556

- Established CUI Program

- Executive Agent (EA) to implement the E.O. and oversee department and agency actions to ensure compliance

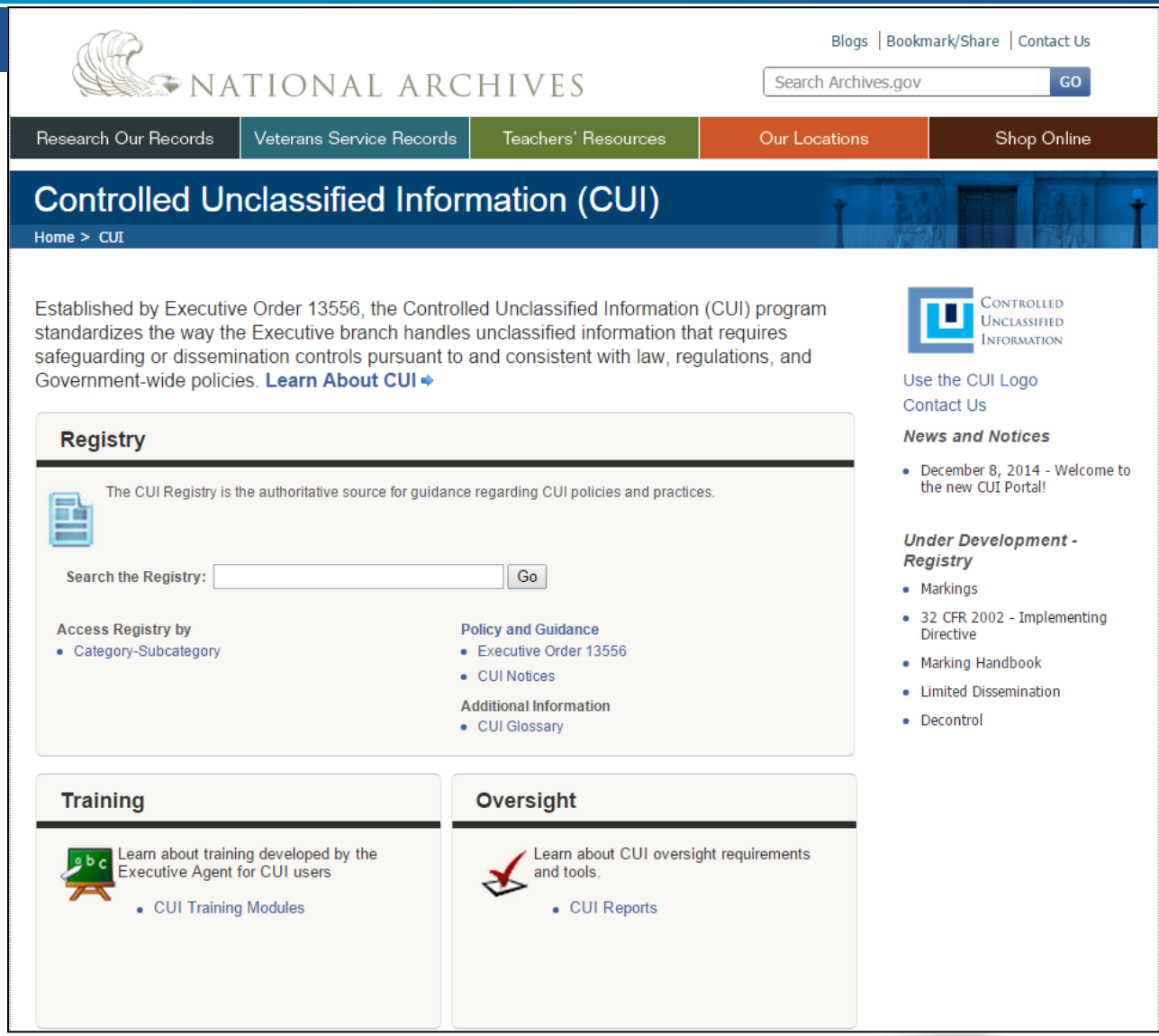


- An open and uniform program to manage all unclassified information within the executive branch that requires safeguarding and dissemination controls as required by law, regulation, and Government-wide policy

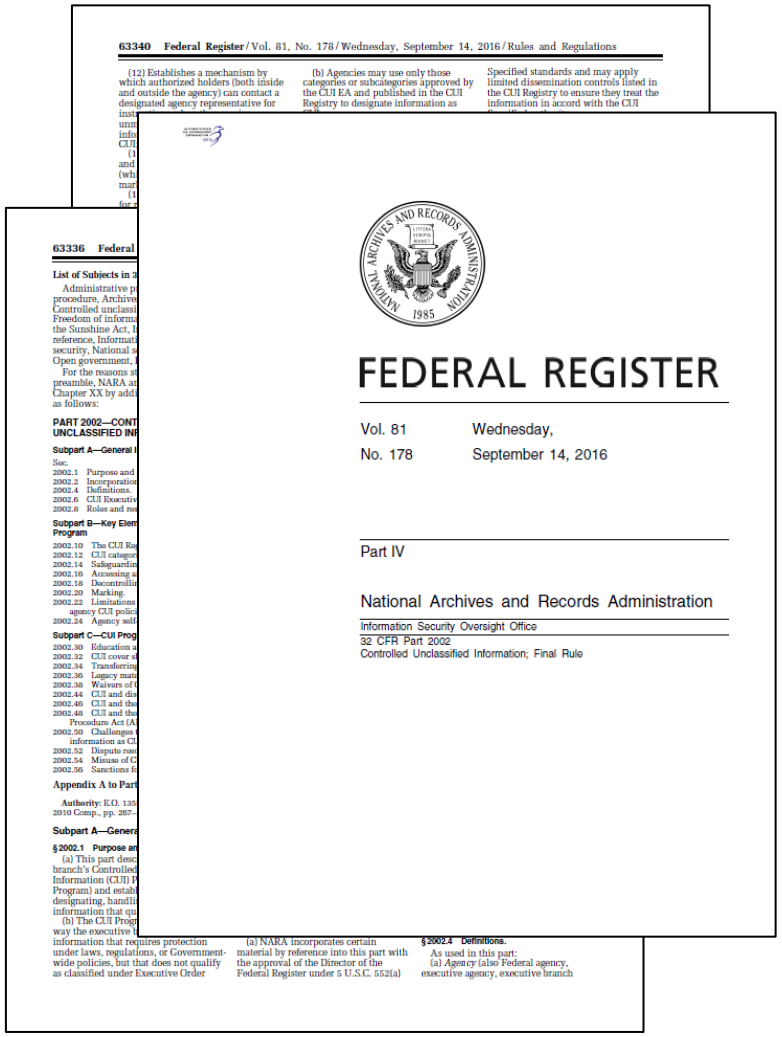
Online Registry

http://www.archives.gov/cui

- 23 Categories
- 84 Sub-categories
- 315 Control citations
- 106 Sanction citations



32 CFR 2002 (September 14, 2016)



- 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 for CUI
  - Physical and Electronic Environments
  - Destruction
  - Marking
  - Sharing
- Emphasizes unique protections described in law, regulation, and/or Government-wide policies (authorities)
  - These protections must continue as described in the underlying authorities.

Two types of CUI: Basic and Specified

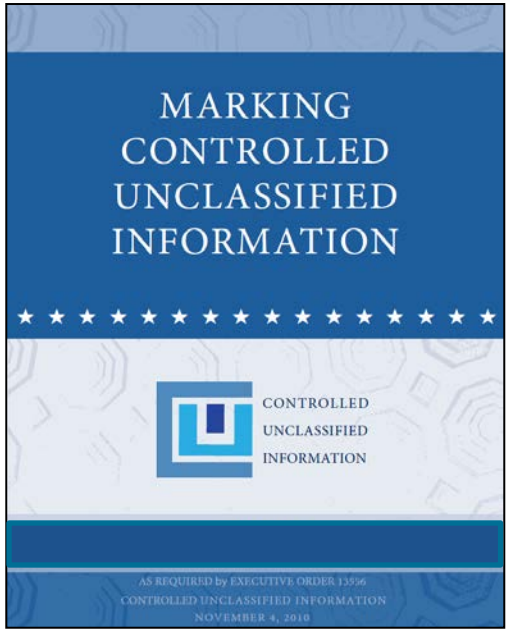
- CUI Basic = LRGWP identifies an information type and says protect it.

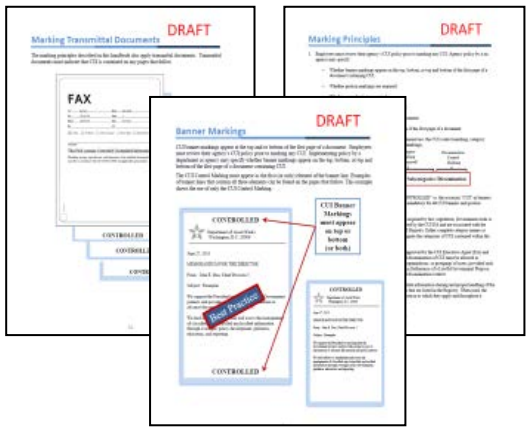
Examples include: Agriculture, Ammonium Nitrate, Water Assessments, Emergency Management, Bank Secrecy, Budget, Comptroller General, Geodetic Product Information, Asylee, Visas, Information Systems Vulnerabilities, Terrorist Screening, Informant, Privilege, Victim, Death Records

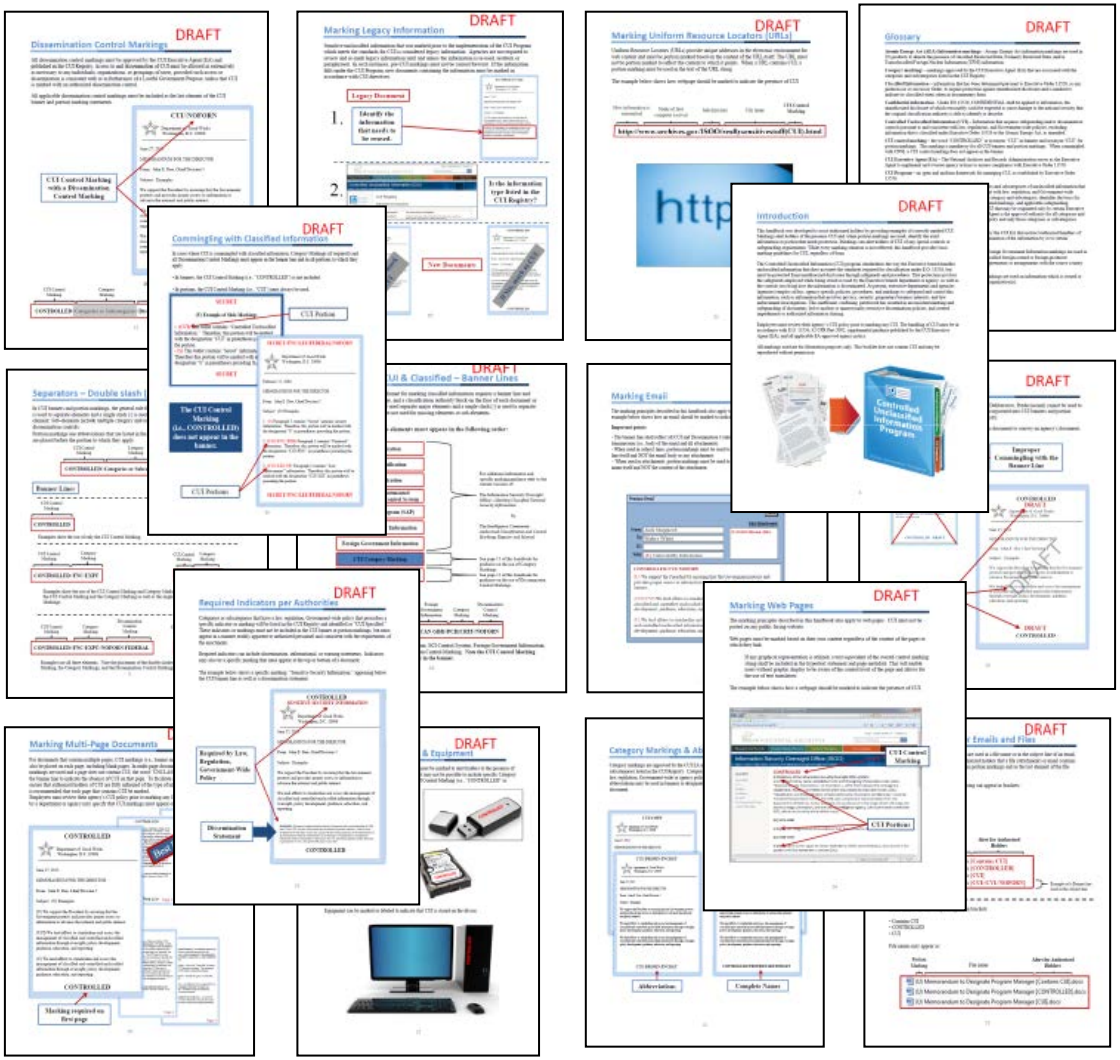
- CUI Specified = LRGWP identifies an information type and says protect it but specifies exactly how it should be protected or handled.

Examples include: Sensitive Security Information, Student Records, Personnel, Source Selection, Nuclear, Safeguards Information, NATO Restricted, NATO Unclassified, Child Pornography, Federal Grand Jury, Witness Protection, DNA, Criminal History Records, Financial Records, Export Control, Protected Critical Infrastructure Information, Controlled Technical Information

Marking Handbook







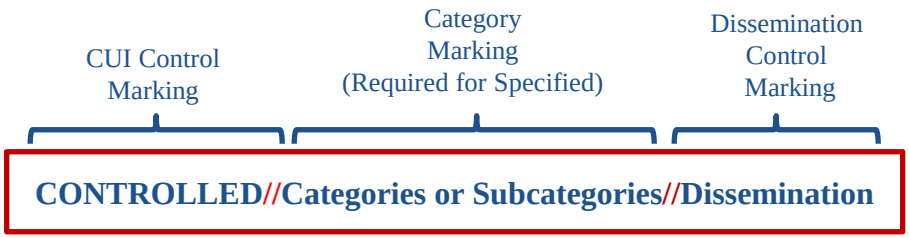
Marking CUI

- 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

Marking CUI: 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.**
- **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.**

Limitations on applicability

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 include additional requirements or restrictions on handling CUI other than those permitted in the Order, the 32 CFR 2002, and the CUI Registry.

Access and Dissemination (Sharing)

Lawful Government purpose is any activity, mission, function, operation, or endeavor that the U.S. Government authorizes or recognizes within the scope of its legal authorities.

Agencies should permit access and dissemination of CUI, provided such access or dissemination:

- Abides by the law, regulation, or Government-wide policy that established the CUI category or subcategory;
- Furthers a Lawful Government Purpose;
- Is not restricted by an authorized limited dissemination control established by the CUI Executive Agent; and,
- Is not otherwise prohibited by law.

General Safeguarding Policy

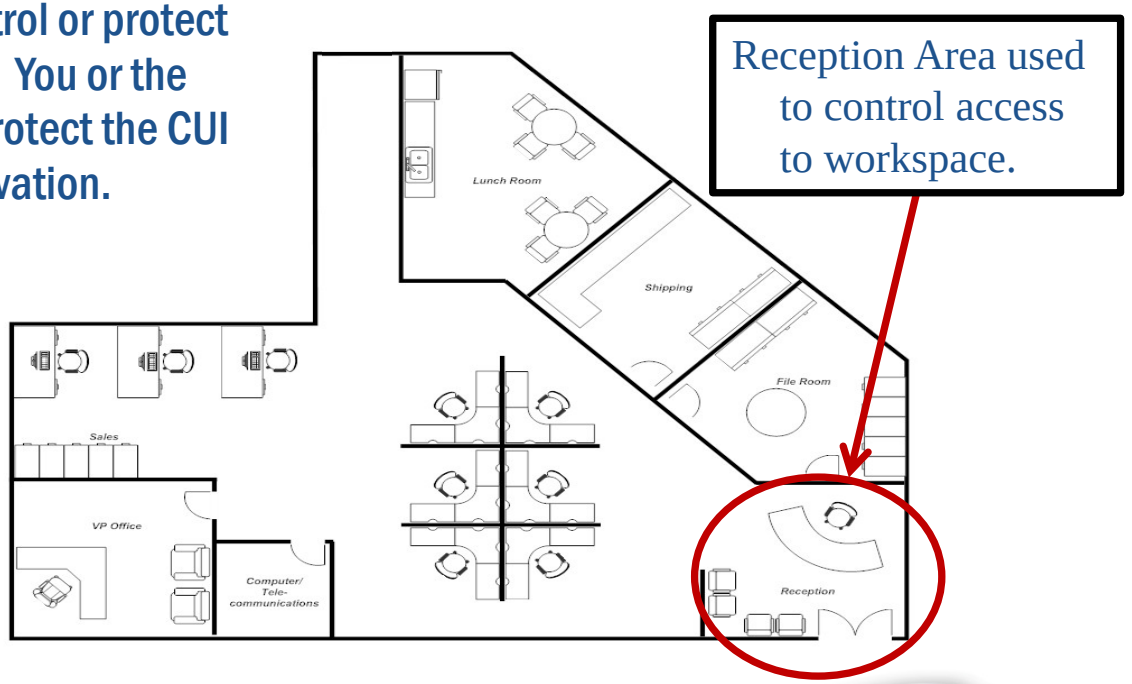
- Agencies must safeguard CUI at all times in a manner that minimizes the risk of unauthorized disclosure while allowing for access by authorized holders.
  - For categories designated as CUI Specified, personnel must also follow the procedures in the underlying law, regulation, or Government-wide policy that established the specific category or subcategory involved.

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

Controlled Environments

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.

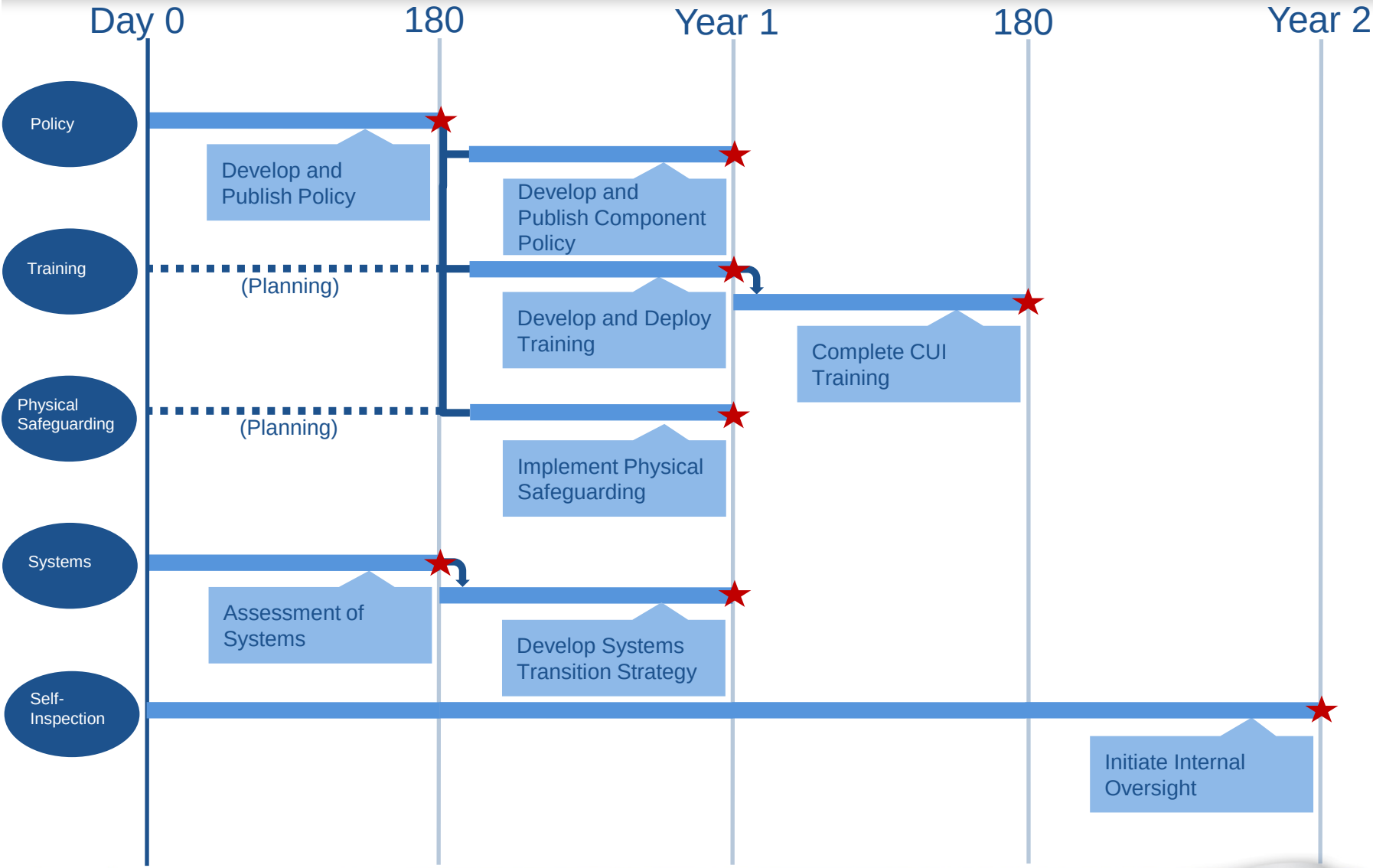
- When outside a controlled environment, you must keep the CUI under your direct control or protect it with at least one physical barrier. You or the physical barrier must reasonably protect the CUI from unauthorized access or observation.



Destruction

- When destroying CUI, including in electronic form, you must do so in a manner that makes it unreadable, indecipherable, and irrecoverable, using any of the following:
  - Guidance for destruction in NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, and NIST SP 800-88, Guidelines for Media Sanitization;
  - Any method of destruction approved for Classified National Security Information, as delineated in 32 CFR 2001.47, Destruction, or any implementing or successor guidance; or
  - Any specific destruction methods required by law, regulation, or Government-wide policy for that item.

Implementation Activities within Executive Branch



Information Systems and CUI

- Purpose of the CUI Program is to provide a uniform and consistent system for protecting CUI throughout executive branch.
- Baseline standard for protecting CUI is no less than moderate confidentiality.
  - Such protection is greater than low, the minimum requirements for all systems under the FISMA
  - Most agencies already configure their systems to Moderate for protection of information falling under the scope of the CUI Program.

Definitions

- All agency heads are responsible for ensuring the protection of Federal information and Federal information systems in accordance with the FISMA.

- *Federal information system* is an information system used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency - 44 USC 3554(a)(1)(A)(ii).

- *On behalf of an agency* occurs when a non-executive branch entity uses or operates an information system or maintains or collects information for the purpose of processing, storing, or transmitting Federal information, and those activities are not incidental to providing a service or product to the Government.

Information Systems Operated on behalf of an Agency

- When a non-Federal stakeholder:
  - 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.

Protections - Operated on behalf of an Agency

- Information systems that a non-executive branch entity operates on behalf of the an agency are subject to CUI requirements as though they are the agency's systems.

- Agencies may require these systems to meet additional requirements the agency sets for its own internal systems.

Information Systems NOT Operated on behalf of an Agency

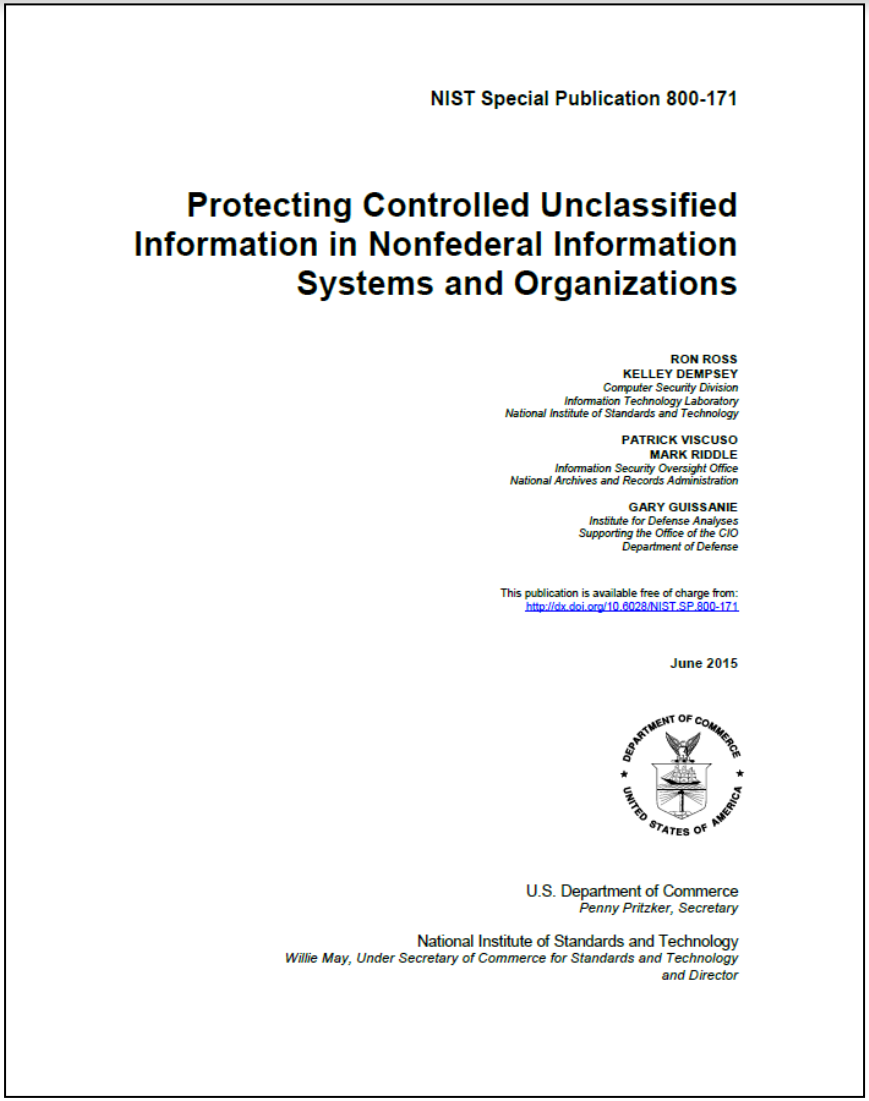
- When a non-Federal stakeholder:
  - Receives CUI incidental to providing a service or product to the Government outside or processing services.
  - Examples: producing a study, conducting research, creating a training program, building an aircraft or ship, providing food services.
- In these instances, the Government is only concerned with the confidentiality of the information;
- And the CUI is regarded as the asset requiring protection.

NIST Special Publication 800-171

This publication provides federal agencies with recommended requirements for protecting the confidentiality of CUI:

(i) when the CUI is resident in nonfederal information systems and organizations;
(ii) when the information systems where the CUI resides are not used or operated by contractors of federal agencies or other organizations on behalf of those agencies; and
(iii) where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or government-wide policy for the CUI category or subcategory listed in the CUI Registry.

The requirements apply to all components of nonfederal information systems and organizations that process, store, or transmit CUI, or provide security protection for such components.



NIST Special Publication 800-171

Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

RON ROSS
KELLEY DEMPSEY
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

PATRICK VISCUSO
MARK RIDDLE
Information Security Oversight Office
National Archives and Records Administration

GARY GUISSANIE
Institute for Defense Analyses
Supporting the Office of the CIO
Department of Defense

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-171

June 2015

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

NIST SP 800-171 and the Cloud

The following will be addressed in a future CUI FAR and are under discussion:

- For CUI processed on a contractor's internal IT system (non- Cloud and/or on an 'internal' Cloud, i.e., the contractor operates its own Cloud system) = NIST SP 800-171.

- For CUI processed on a contractor's internal IT system BUT the contractor is also outsourcing some of the CUI processing to an external Cloud Service Provider (CSP) (e.g., Microsoft, Amazon) = NIST SP 800-171 for the contractor's internal IT system and FedRAMP Moderate-equivalent protections in the CSP's Cloud.

Development of 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.
- Starting with the FIPS Publication 200 security requirements and the security controls in the **moderate baseline** (i.e., the minimum level of protection required for CUI in federal information systems and organizations), the requirements and controls are *tailored to eliminate requirements, controls, or parts of controls that are:*

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.**

Security Requirements: 14 Families

- ✓ Access Control.
- ✓ Audit and Accountability.
- ✓ Awareness and Training.
- ✓ Configuration Management.
- ✓ Identification and Authentication.
- ✓ Incident Response.
- ✓ Maintenance.
- ✓ Media Protection.
- ✓ Physical Protection.
- ✓ Personnel Security.
- ✓ Risk Assessment.
- ✓ Security Assessment.
- ✓ System and Communications Protection
- ✓ System and Information Integrity.

Obtained from FIPS 200 and NIST Special Publication 800-53.

Moderate Baseline (Select Controls)

Access Control, 3.1.13, Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.

Awareness and Training, 3.2.3, Provide security awareness training on recognizing and reporting potential indicators of insider threat.

Audit and Accountability, 3.3.2, Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

Incident Response, 3.6.1, Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.

Media Protection:

3.8.1, Protect (i.e., physically control and securely store) information system media containing CUI, both paper and digital.

3.8.3, Sanitize or destroy information system media containing CUI before disposal or release for reuse.

Moderate Baseline (Select Controls)

Physical Protection, 3.10.1, Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

Identification and Authentication, 3.5.3, Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.

- Multifactor authentication requires two or more different factors to achieve authentication. Factors include: (i) something you know (e.g., password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric).

- The requirement for multifactor authentication should not be interpreted as requiring federal Personal Identity Verification (PIV) card or Department of Defense Common Access Card (CAC)-like solutions. A variety of multifactor solutions (including those with replay resistance) using tokens and biometrics are commercially available. Such solutions may employ hard tokens (e.g., smartcards, key fobs, or dongles) or soft tokens to store user credentials.

Moderate Baseline (Select Controls)

System and Information Integrity:

3.14.6, Monitor the information system including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

3.14.7, Identify unauthorized use of the information system.

Security Assessment, 3.12.3, Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

Moderate Baseline (Select Controls)

Systems and Communications Protection:

3.13.8, Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.

3.13.11, Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.

- ❑ A cryptographic module validated by the Cryptographic Module Validation Program (CMVP) to meet requirements specified in FIPS Publication 140-2 (as amended). As a prerequisite to CMVP validation, the cryptographic module is required to employ a cryptographic algorithm implementation that has successfully passed validation testing by the Cryptographic Algorithm Validation Program (CAVP).

Structure of NIST SP 800-171

- Basic Security Requirements & Derived Security Requirements
- Tables that illustrate the mapping of CUI requirements to security controls in:
  - National Institute of Standards and Technology Special Publication (NIST SP) 800-53
  - International Organization for Standardization / International Electrotechnical Commission (ISO/IEC) 27001

CUI SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.1 ACCESS CONTROL				
Basic Security Requirements				
3.1.1 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). **3.1.2** Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	AC-2	Account Management	A.9.2.1	User registration and de-registration
			A.9.2.2	User access provisioning
			A.9.2.3	Management of privileged access rights
			A.9.2.5	Review of user access rights
			A.9.2.6	Removal or adjustment of access rights
	AC-3	Access Enforcement	A.6.2.2	Teleworking
			A.9.1.2	Access to networks and network services
			A.9.4.1	Information access restriction
			A.9.4.4	Use of privileged utility programs
			A.9.4.5	Access control to program source code
			A.13.1.1	Network controls
			A.14.1.2	Securing application services on public networks
			A.14.1.3	Protecting application services transactions
			A.18.1.3	Protection of records
	AC-17	Remote Access	A.6.2.1	Mobile device policy
			A.6.2.2	Teleworking
			A.13.1.1	Network controls
			A.13.2.1	Information transfer policies and procedures
			A.14.1.2	Securing application services on public networks
Derived Security Requirements				
3.1.3 Control the flow of CUI in accordance with approved authorizations.	AC-4	Information Flow Enforcement	A.13.1.3	Segregation in networks
			A.13.2.1	Information transfer policies and procedures
			A.14.1.2	Securing application services on public networks
			A.14.1.3	Protecting application services transactions

CUI Approach for Contractor Environment

Government

E.O. 13556

Registry

32 CFR 2002

NIST SP 800-171

FAR

Industry

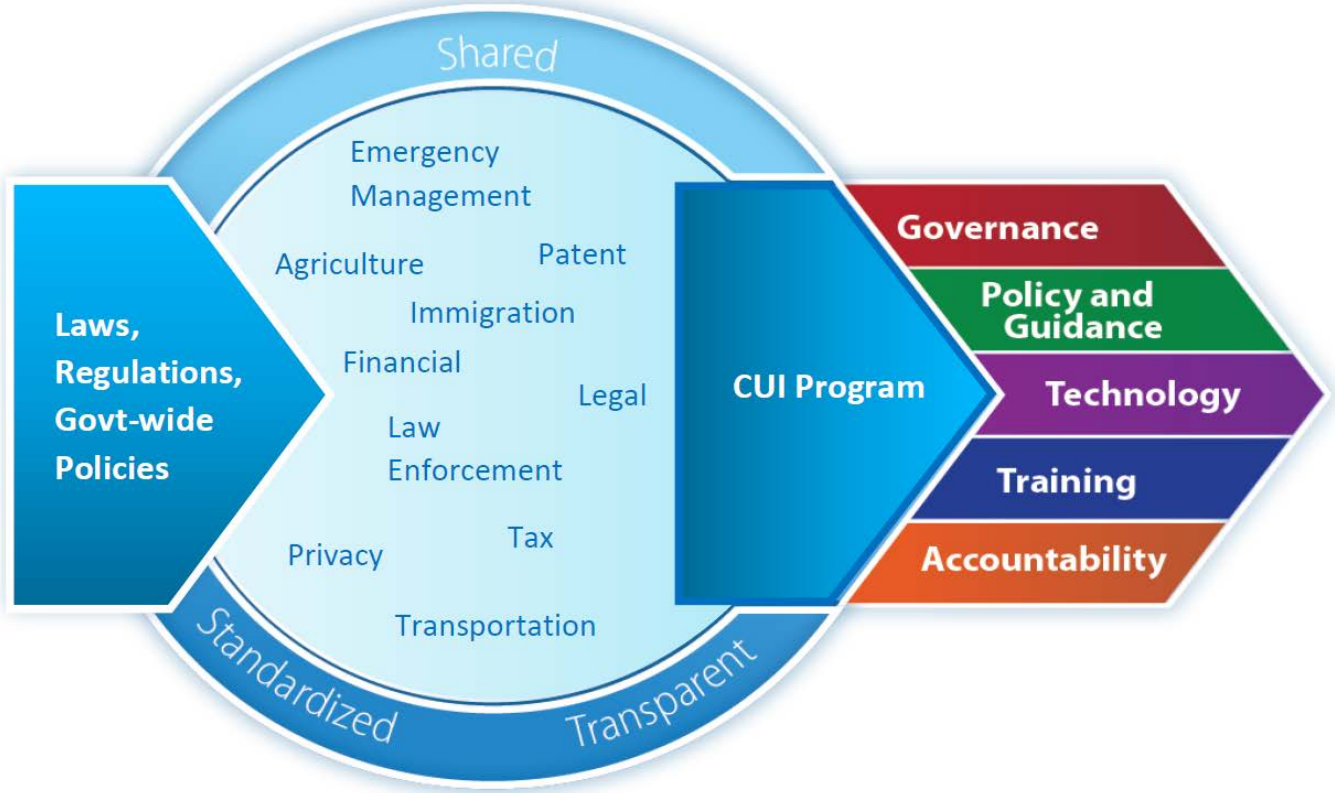
1 Year

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.

Discussion points for future CUI FAR

- Identification and marking of all information requiring protection.
- Identification of all CUI categories/subcategories and any CUI Specified requirements.
- Oversight approach – certification; certification with documentation; and certification/documentation with validation (inspection).
  - Possible use of System for Acquisition Management in all three instances.
- Breaches and contractual liability.
- NIST SP 800-171 under revision to include SSP/POAM.
- Federally funded research.

Questions?


Shared
Emergency Management
Agriculture
Patent
Immigration
Financial
Legal
Law Enforcement
Privacy
Tax
Transportation
Standardized
Transparent
Laws, Regulations, Govt-wide Policies
CUI Program
Governance
Policy and Guidance
Technology
Training
Accountability