Special Publication 800-171

Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

Dr. Ron Ross
Computer Security Division
Information Technology Laboratory

First, some definitions.

Controlled Unclassified Information

Information that law, regulation, or governmentwide policy requires to have safeguarding or disseminating controls, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended.

-- Executive Order 13556

Controlled Unclassified Information

Supports federal missions and business functions…

…that affect the economic and national security interests of the United States.

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 Organization

An entity that owns, operates, or maintains a nonfederal information system.

-- NIST Special Publication 800-171

Nonfederal Organizations

Some Examples

- Federal contractors.
- State, local, and tribal governments.
- Colleges and universities.

An urgent need…
A national imperative.

The protection of Controlled Unclassified Information while residing in nonfederal information systems and organizations is of paramount importance to federal agencies and can *directly* impact the ability of the federal government to successfully carry out its designated missions and business operations.

-- NIST Special Publication 800-171

Executive Order 13556

Controlled Unclassified Information

November 4, 2010

The Order —

- Established a governmentwide Controlled Unclassified Information (CUI) Program to standardize the way the Executive branch handles unclassified information that requires protection.
- Designated the National Archives and Records Administration (NARA) as the Executive Agent to implement the CUI program.

Only information that requires safeguarding or dissemination controls pursuant to federal law, regulation, or governmentwide policy may be designated as CUI.

The CUI Registry

www.archives.gov/cui/registry/category-list.html

- Online repository for information, guidance, policy, and requirements on handling CUI, including issuances by the CUI Executive Agent.
- Identifies approved CUI categories and subcategories (with descriptions of each) and the basis for controls.
- Sets out procedures for the use of CUI, including but not limited to marking, safeguarding, transporting, disseminating, re-using, and disposing of the information.

The Big Picture

A three-part plan for the protection of CUI

- 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.

NIST Special Publication 800-171

Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

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.***

Target Audience

Public and Private Sectors

Individuals with —

- System development life cycle responsibilities.
  - Program managers, information owners, mission/business owners.
- Acquisition or procurement responsibilities.
  - Contracting officers, COTRs.
- Information security or risk management responsibilities.
  - Authorizing officials, CIOs, CISOs, system owners/security managers.
- Security assessment and monitoring responsibilities.
  - Auditors, system evaluators, assessors, independent verifiers and validators.

Assumption #1

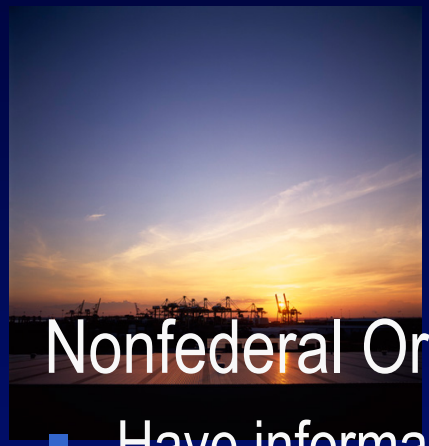
- Statutory and regulatory requirements for the protection of CUI are *consistent*, whether such information resides in federal information systems or nonfederal information systems.

Assumption #2

- Safeguards implemented to protect CUI are *consistent* in both federal and nonfederal information systems and organizations.

Assumption #3

- The confidentiality impact value for CUI is no lower than *moderate* 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.

CUI Security Requirements

Basic and derived security requirements are obtained from FIPS 200 and NIST SP 800-53 initially — and then *tailored* appropriately to *eliminate* requirements that are:

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

Security Requirements

14 Families

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

- 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.

Structure of Security Requirements

- Security requirements have a well-defined structure that consists of the following components:
  - ***Basic security requirements section.***
  - ***Derived security requirements section.***

Security Requirement

Configuration Management Example

Basic Security Requirements:

3.4.1 Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational information systems.

Derived Security Requirements:

3.4.3 Track, review, approve/disapprove, and audit changes to information systems.

3.4.4 Analyze the security impact of changes prior to implementation.

3.4.5 Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.

Mapping CUI Requirements to ISO 27001 and SP 800-53 Security Controls

Mapping Tables.

Two new appendices.

Tailoring actions applied to moderate security control baseline.

Tailoring Criteria.

Appendix E

TAILORING SYMBOL	TAILORING CRITERIA
NCO	NOT DIRECTLY RELATED TO PROTECTING THE CONFIDENTIALITY OF CUI.
FED	UNIQUELY FEDERAL, PRIMARILY THE RESPONSIBILITY OF THE FEDERAL GOVERNMENT.
NFO	EXPECTED TO BE ROUTINELY SATISFIED BY NONFEDERAL ORGANIZATIONS WITHOUT SPECIFICATION.
CUI	THE CUI BASIC OR DERIVED SECURITY REQUIREMENT IS REFLECTED IN AND IS TRACEABLE TO THE SECURITY CONTROL, CONTROL ENHANCEMENT, OR SPECIFIC ELEMENTS OF THE CONTROL/ENHANCEMENT.

Appendix E – AC Family

	NIST SP 800-53 MODERATE BASELINE SECURITY CONTROLS	
AC-1	Access Control Policy and Procedures	NFO
AC-2	Account Management	CUI
AC-2(1)	*ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT*	NCO
AC-2(2)	*ACCOUNT MANAGEMENT | REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS*	NCO
AC-2(3)	*ACCOUNT MANAGEMENT | DISABLE INACTIVE ACCOUNTS*	NCO
AC-2(4)	*ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS*	NCO
AC-3	Access Enforcement	CUI
AC-4	Information Flow Enforcement	CUI
AC-5	Separation of Duties	CUI
AC-6	Least Privilege	CUI
AC-6(1)	*LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS*	CUI
AC-6(2)	*LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS*	CUI

Appendix E – CM Family

	NIST SP 800-53 MODERATE BASELINE SECURITY CONTROLS	
CM-1	Configuration Management Policy and Procedures	NFO
CM-2	Baseline Configuration	CUI
CM-2(1)	*BASELINE CONFIGURATION | REVIEWS AND UPDATES*	NFO
CM-2(3)	*BASELINE CONFIGURATION | RETENTION OF PREVIOUS CONFIGURATIONS*	NCO
CM-2(7)	*BASELINE CONFIGURATION | CONFIGURE SYSTEMS, COMPONENTS, OR DEVICES FOR HIGH-RISK AREAS*	NFO
CM-3	Configuration Change Control	CUI
CM-3(2)	*CONFIGURATION CHANGE CONTROL | TEST / VALIDATE / DOCUMENT CHANGES*	NFO
CM-4	Security Impact Analysis	CUI
CM-5	Access Restrictions for Change	CUI
CM-6	Configuration Settings	CUI
CM-7	Least Functionality	CUI
CM-7(1)	*LEAST FUNCTIONALITY | PERIODIC REVIEW*	CUI

Appendix E – CA Family

	NIST SP 800-53 MODERATE BASELINE SECURITY CONTROLS	
CA-1	Security Assessment and Authorization Policies and Procedures	NFO
CA-2	Security Assessments	CUI
CA-2(1)	*SECURITY ASSESSMENTS | INDEPENDENT ASSESSORS*	NFO
CA-3	System Interconnections	NFO
CA-3(5)	*SYSTEM INTERCONNECTIONS | RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS*	NFO
CA-5	Plan of Action and Milestones	CUI
CA-6	Security Authorization	FED
CA-7	Continuous Monitoring	CUI
CA-7(1)	*CONTINUOUS MONITORING | INDEPENDENT ASSESSMENT*	NFO
CA-9	Internal System Connections	NFO

The road ahead.

In the Interim…

Using NIST Special Publication 800-171 on a voluntary basis

- Until the formal process of establishing a single FAR clause takes place, the CUI security requirements in NIST Special Publication 800-171 may be referenced in federal contracts consistent with federal law and regulatory requirements.


We The People

Contact Information

100 Bureau Drive Mailstop 8930
Gaithersburg, MD USA 20899-8930

NIST

Dr. Ron Ross
(301) 975-5390
ron.ross@nist.gov

NIST

Kelley Dempsey
(301) 975-2827
kelley.dempsey@nist.gov

NARA/ISOO

Dr. Pat Viscuso
(202) 357-5313
patrick.viscuso@nara.gov

NARA/ISOO

Mark Riddle
(202) 357-6864
mark.riddle@nara.gov

Comments: sec-cert@nist.gov

Web: csrc.nist.gov