NIST Special Publication 800-171:
Protecting CUI in Nonfederal Information Systems and Organizations

Federal Computer Security Manager's Forum

August 16th, 2016

Kelley Dempsey
NIST IT Laboratory
Computer Security Division

What is 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 (CUI)

Supports federal missions and business functions that affect the economic and national security interests of the United States.

Executive Order 13556

Controlled Unclassified Information

November 4, 2010

- 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.

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

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.

-- CUI Regulation (32 CFR Part 2002)

Nonfederal Organization

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

-- NIST Special Publication 800-171

Nonfederal Organizations

Some Potential Examples

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

The Big Picture

A three-part plan for the protection of CUI

- Federal CUI rule (32 CFR Part 2002) establishes the required controls and markings for CUI governmentwide.
- NIST Special Publication 800-171 defines 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 SP 800-171 to nonfederal organizations (planned for 2017).

CUI Regulation: *What Does It Say?*

- Codifies that CUI is at least moderate for C
- Defines "on behalf of an agency"
- Information systems that process, store, or transmit CUI may be *federal* or *nonfederal*
  - When *federal* (including contractors operating *on behalf of*), agency security requirements are applied (i.e., FISMA/RMF)
  - When *nonfederal*, SP 800-171 security requirements are applied

On Behalf of an Agency…

From the CUI Regulation (section 2002.4):

"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."

Purpose of SP 800-171

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 nonfederal organization is ***not*** collecting or maintaining information **on behalf of** a federal agency OR using or operating an information system **on behalf of** a federal agency.**

Applicability of SP 800-171

- 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.

Three Primary Assumptions

1. Statutory and regulatory requirements for the protection of CUI are ***consistent***, whether such information resides in federal information systems or nonfederal information systems.
2. Safeguards implemented to protect CUI are ***consistent*** in both federal and nonfederal information systems and organizations.
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 controls 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 from FIPS 200
- Derived security requirements from SP 800-53

Security Requirement

Configuration Management Example

Basic Security Requirements (FIPS 200):

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 (SP 800-53):

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.

Tying it Together: Two Important Appendices

- Appendix D - Mapping Tables - Maps SP 800-171 to ISO 27001 and SP 800-53 Security Controls
- Appendix E - Tailoring Criteria - Tailoring actions applied to the moderate security control baseline
  - NCO – Not related to protecting Confidentiality
  - FED – Uniquely federal/responsibility of government
  - NFO – Expected to be satisfied w/o specification
  - CUI – Security requirement in SP 800-171

Revision 1 (DRAFT)

- Public comment period: Aug 16 – Sept 16 2016
- Minor change to purpose (as noted on slide 14) and clarified footnote regarding FISMA
- "Proposed" language removed from references to the CUI Regulation.
- Use of parameters from SP 800-53 available for use by nonfederal organizations when implementing SP 800-171 security requirements.
- Added requirement for SSP development
- Minor clarifications, additions to glossary, etc.

Contact Information

Project Leader and NIST Fellow

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

Senior Information Security Specialist

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

Administrative Support

Peggy Himes
(301) 975-2489
peggy.himes@nist.gov

Information Security Specialists

Ned Goren
(301) 975-5233
nedim.goren@nist.gov

Michael Nieles
(301) 975-2228
michael.nieles@nist.gov

Comments: sec-cert@nist.gov (goes to all of the above)

Web: http://csrc.nist.gov/groups/SMA/fisma/