NIST Special Publication 800-171

Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

Published: June 2015

Kelley Dempsey
Computer Security Division
Information Technology Laboratory

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

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

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.

Basic Principles

- The confidentiality impact value for CUI is no lower than *moderate* in accordance with FIPS Publication 199.
- Facilitate *consistency* in the statutory and regulatory requirements for the protection of CUI, whether such information resides in federal information systems or nonfederal information systems.
- Facilitate *consistency* in the safeguards implemented to protect CUI in both federal and nonfederal information systems and organizations.

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 already 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 Requirements

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.

Helpful Appendices

Appendix D - Mapping Tables

Provides a mapping of CUI Requirements to ISO 27001 and SP 800-53 Security Controls

Appendix E - Tailoring Criteria.

Provides details on how tailoring actions were applied to moderate security control baseline.

NIST Contact Information

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

Dr. Ron Ross

301 975-5390
ron.ross@nist.gov

Kelley Dempsey

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

Questions/Comments: sec-cert@nist.gov

Web: http://csrc.nist.gov