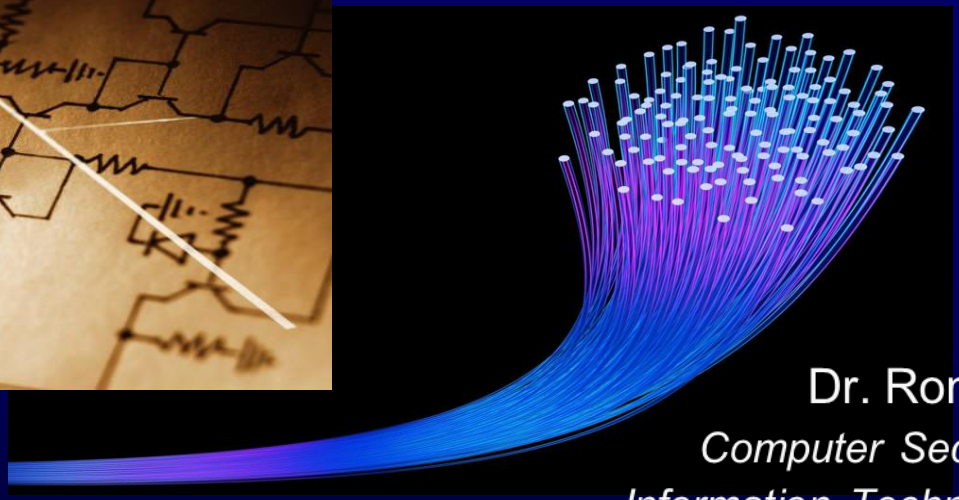
Information System Security Association-Washington D.C.

NIST 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 requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, excluding information that is classified under Executive Order 13526 of December 29, 2009, or the Atomic Energy Act, as amended.

-- E.O. 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 SP 800-171

Nonfederal Organization

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

-- NIST SP 800-171

Nonfederal Organizations

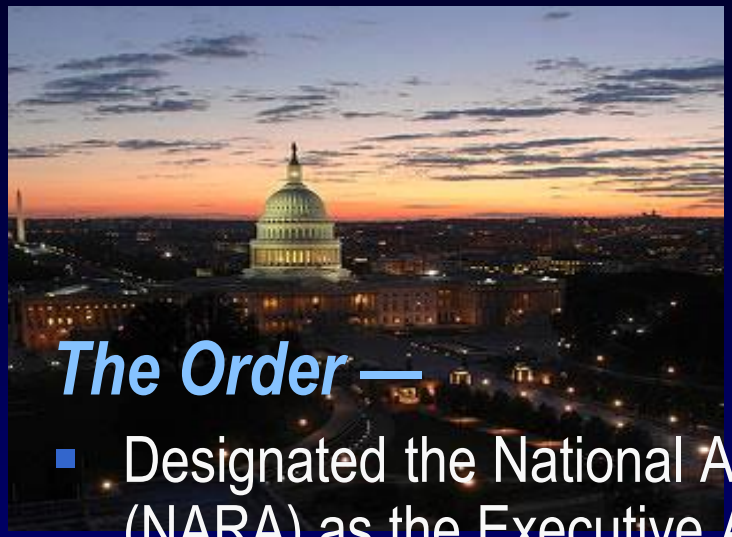
Some Examples

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

An urgent need…
A national imperative.

The protection of sensitive, unclassified federal information while residing in nonfederal information systems and environments of operation 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 SP 800-171



Executive Order 13556

Controlled Unclassified Information

November 10, 2010

The Order —

- Designated the National Archives and Records Administration (NARA) as the Executive Agent for Controlled Unclassified Information (CUI).
- Directed NARA to implement a governmentwide CUI Program to standardize the way the Executive branch handles unclassified information that requires protection.
- Established an open and uniform program to manage unclassified information within the executive branch that requires safeguarding and dissemination controls as required by law, regulation, and Government-wide policy.

CUI Registry

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

- Identifies the exclusive categories and subcategories of unclassified information that require safeguarding and dissemination controls consistent with law, federal regulation, and Government-wide policies.
- Serves as the central repository for the posting of and access to the categories and subcategories, associated markings, and applicable safeguarding, dissemination, and decontrol procedures.

The Big Picture

A three-part plan for the protection of CUI

- Development of 32 CFR Part 2002.
- Development of NIST SP 800-171.
- Development of single Federal Acquisition Regulation (FAR) Clause.

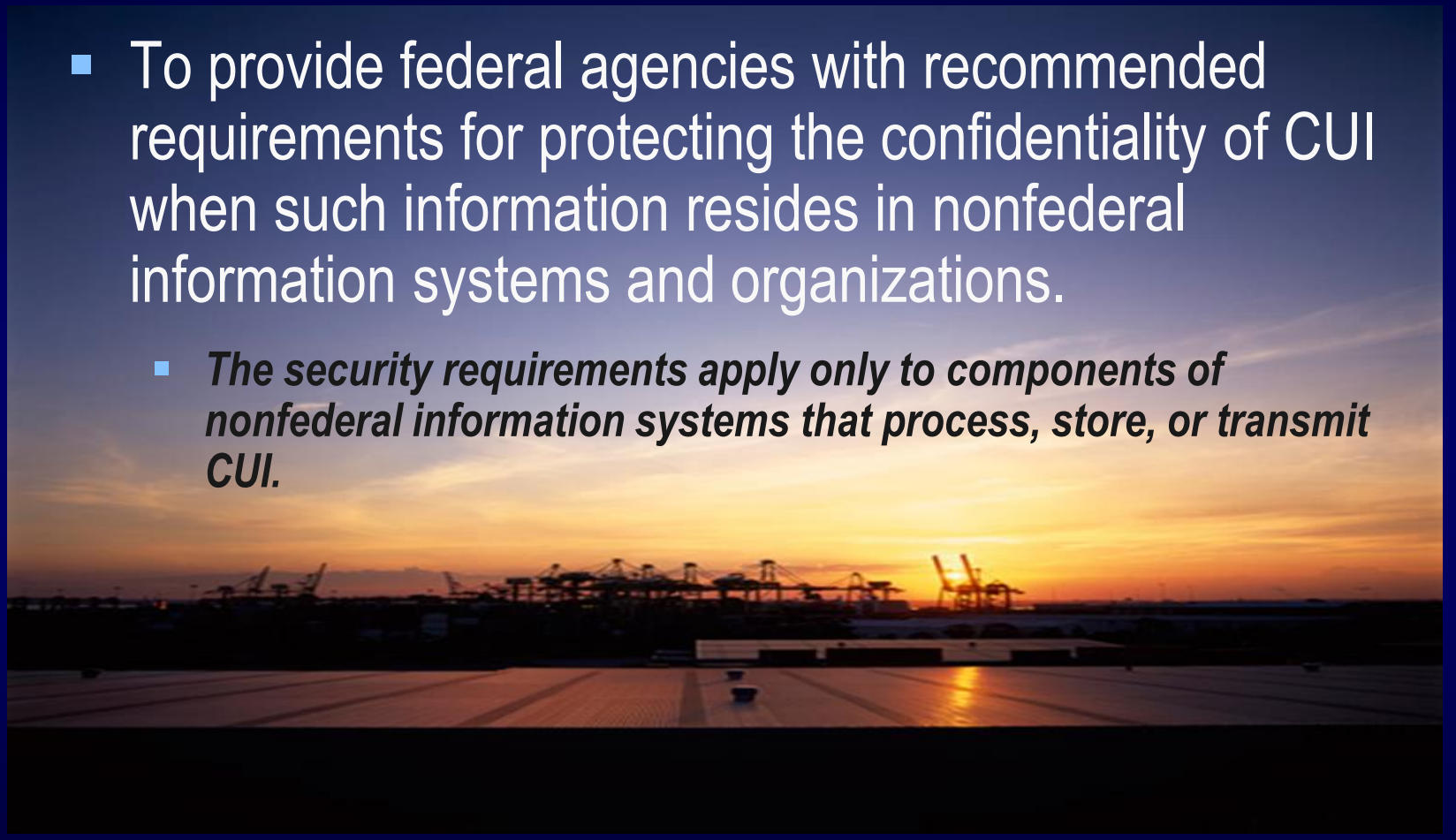
NIST Special Publication 800-171

Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

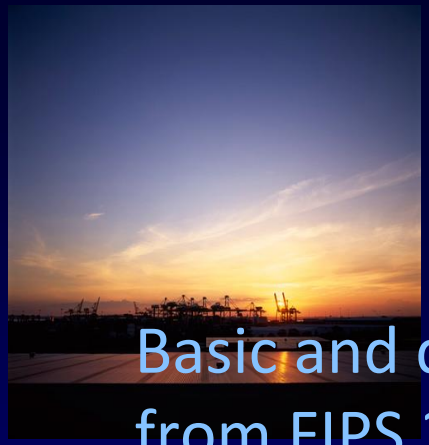
Initial Public Draft

November 2014

Purpose and Applicability



- To provide federal agencies with recommended requirements for protecting the confidentiality of CUI when such information resides in nonfederal information systems and organizations.
  - ***The security requirements apply only to components of nonfederal information systems that process, store, or transmit 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:

- Primarily the responsibility of the federal government (i.e., uniquely federal requirements).
- Related primarily to availability.
- Assumed to be routinely satisfied by nonfederal organizations without any further specification.

Target Audience

- Individuals with system development life cycle responsibilities.
  - Program managers, information owners, mission/business owners, system owners, acquisition officials.
- Individuals with information system, security, or risk management and oversight responsibilities.
  - Authorizing officials, chief information officers, chief information security officers, information system/security managers.
- Individuals with security assessment and monitoring responsibilities.
  - Auditors, system evaluators, assessors, independent verifiers and validators, analysts.

Assumption #1

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

Assumption #2

- Safeguards or countermeasures implemented to protect CUI are consistent in both federal and nonfederal environments.

Assumption #3

- The confidentiality impact value for CUI is no lower than *moderate* in accordance with Federal Information Processing Standards (FIPS) Publication 199.

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 requirement section.***
  - ***Derived security requirements section.***
  - ***References section.***

Security Requirement

Configuration Management Example

Basic Security Requirement: Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and establish and enforce security configuration settings for information technology products employed in organizational information systems.

Derived Security Requirements:

a. Analyze the security impact of changes prior to implementation;
b. Employ the principle of least functionality by configuring the information system to provide only essential capabilities;
c. Restrict, disable, and prevent the use of nonessential functions, ports, protocols, and services; and
d. Apply deny by exception (blacklist) policy to prevent the use of unauthorized software.

References: NIST Special Publication 800-53.

Configuration Management	**CM-2; CM-4; CM-5; CM-6; CM-7; CM-7(1); CM-7(2); CM-7(4); CM-8.**

The road ahead.

On the Horizon…

Proposed 32 CFR Part 2002, Controlled Unclassified Information

- NARA is issuing a Federal regulation, or directive (currently in coordination with OMB), to establish the required CUI security controls and markings governmentwide.
- Requirements for the protection of CUI at the *moderate* confidentiality impact value in the proposed rule are based on applicable governmentwide standards and guidelines issued by NIST, and applicable policies established by OMB.

On the Horizon…

Standard Federal Acquisition Regulation (FAR) Clause

- The CUI Executive Agent also anticipates establishing a single Federal Acquisition Regulation (FAR) clause that will apply the requirements of the proposed CUI rule and NIST SP 800-171 to contractor environments.
- This will further promote standardization to help nonfederal organizations meet the current range and types of contract clauses, where differing requirements and conflicting guidance from federal agencies gives rise to confusion and inefficiencies.

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, and where necessitated by exigent circumstances, NIST SP 800-171 may be referenced in contract specific requirements on a limited basis—consistent with acquisition and regulatory requirements.

NIST Special Publication 800-171
Public Comment Period

November 18, 2014 – January 16, 2015

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory

100 Bureau Drive (Mail Stop 8930)
Gaithersburg, MD 20899-8930

Copies available at: csrc.nist.gov
Send comments to: sec-cert@nist.gov


We The People

Contact Information

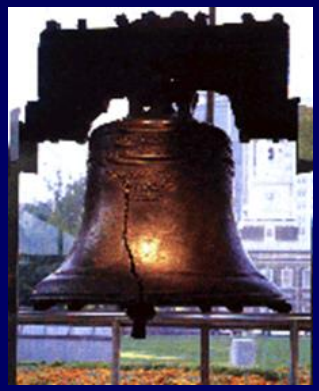
100 Bureau Drive Mailstop 8930
Gaithersburg, MD USA 20899-8930

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