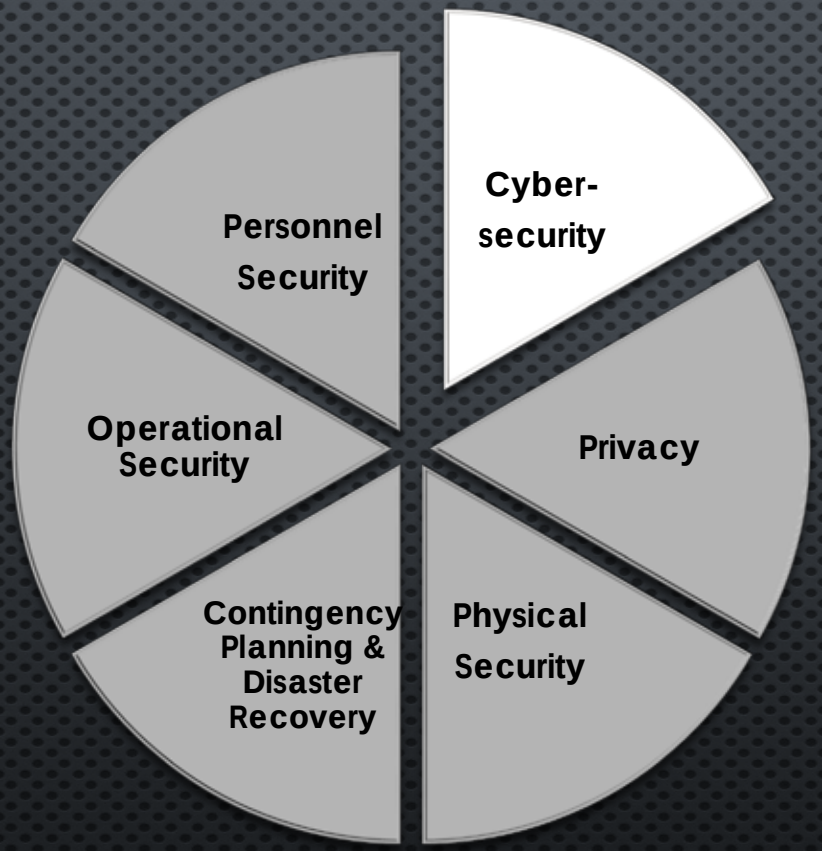
NIST Special Publication 800-171

Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

Ryan Bonner
Brightline

WHAT IS INFORMATION SECURITY?



NONFEDERAL ORGANIZATIONS

SOME EXAMPLES

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

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.

CUI REGISTRY

- MANUFACTURING

Category-Subcategory:	**Proprietary Business Information-Manufacturer**
Category Description:	Material and information relating to, or associated with, a company's products, business, or activities, including but not limited to financial information; data or statements; trade secrets; product research and development; existing and future product designs and performance specifications.
Subcategory Description:	Relating to the production of a consumer product to include that of a private labeler.
Marking:	MFC

The Big Picture

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
- DFAR clause 252.204.7008 requires compliance to 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.*

ASSUMPTIONS

Nonfederal Organizations —

- Have information technology infrastructures in place
  - 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

NIST Special Publication 800-171 Rev 1

Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

December 2016

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf

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.

3.4.5 .....

Security Requirement

Configuration Management Example 3.4.1

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.

Meeting the Requirements:

- Develops, documents and maintains a current baseline configuration of the information system
- Configuration control in place

Security Requirement

Configuration Management Example 3.4.1

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.

Meeting the Requirements:

- Configuration management policy; procedures and plan.
- Documentation for Enterprise architecture or information system design.
- Information system configuration settings and associated documentation.
- Change control records.
- Personnel with configuration management responsibilities.
- System/network administrator.

DFARS 252.204.7008

"If the Offeror proposes to vary from any of the security requirements specified by NIST SP 800-171 that are in effect at the time the solicitation is issued or as authorized by the Contracting Officer, the Offeror shall submit to the Contracting Officer, for consideration by the DoD Chief Information Officer (CIO), a written explanation of—

(A) Why a particular security requirement is not applicable; or

(B) How an alternative but equally effective, security measure is used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection."

MEETING SP 800-171

- Some security controls may not be applicable to your environment
- Build off what you are currently doing
- Other ways to meet the requirements

MEETING SP 800-171

- MORE COST EFFECTIVE APPROACH
  - ISOLATE CUI INTO ITS OWN SECURITY DOMAIN BY APPLYING ARCHITECTURAL DESIGN CONCEPTS
  - SECURITY DOMAINS MAY EMPLOY PHYSICAL SEPARATION, LOGICAL SEPARATION, OR A COMBINATION OF BOTH
  - USE THE SAME CUI INFRASTRUCTURE FOR MULTIPLE GOVERNMENT CONTRACTS OR AGREEMENTS

MEETING SP 800-171

BIGGEST CONTRIBUTORS TOWARDS COMPLIANCE

- CUSTOMIZED WINDOWS DOMAIN NETWORK
  - UP TO 35 REQUIREMENTS MET
- ROBUST POLICIES
  - UP TO 27 REQUIREMENTS MET
- CONTINUOUS MONITORING PLATFORM
  - UP TO 18 REQUIREMENTS MET
- ENDPOINT SECURITY SOFTWARE (REPLACES TRADITIONAL ANTIVIRUS)
  - UP TO 18 REQUIREMENTS MET
- NEXT-GEN FIREWALL
  - UP TO 15 REQUIREMENTS MET