NIST Special Publication 800-171

Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

David Stieren
Programs and Partnerships Division
NIST MEP

June 2017

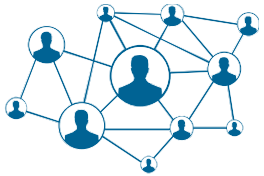
on behalf of Pat Toth
NIST MEP Cybersecurity Program Manager

NIST Manufacturing Extension Partnership (MEP)

NIST National Institute of Standards and Technology U.S. Department of Commerce

PROGRAM MISSION

To enhance the productivity and technological performance of U.S. Manufacturing



National Network

- MEP Center in all 50 U.S. states plus Puerto Rico.
- System-wide non-Federal staff of over 1,200 individuals in ~600 service locations assisting U.S. manufacturers.
- Contracting with >2,500 3rd party service providers

Local ➡ National Connection

System of Centers providing localized service to manufacturers in each State – with National reach and resources

MEP Budget & Business Model

$130M FY17 Federal Budget with Cost Share Requirements for Centers

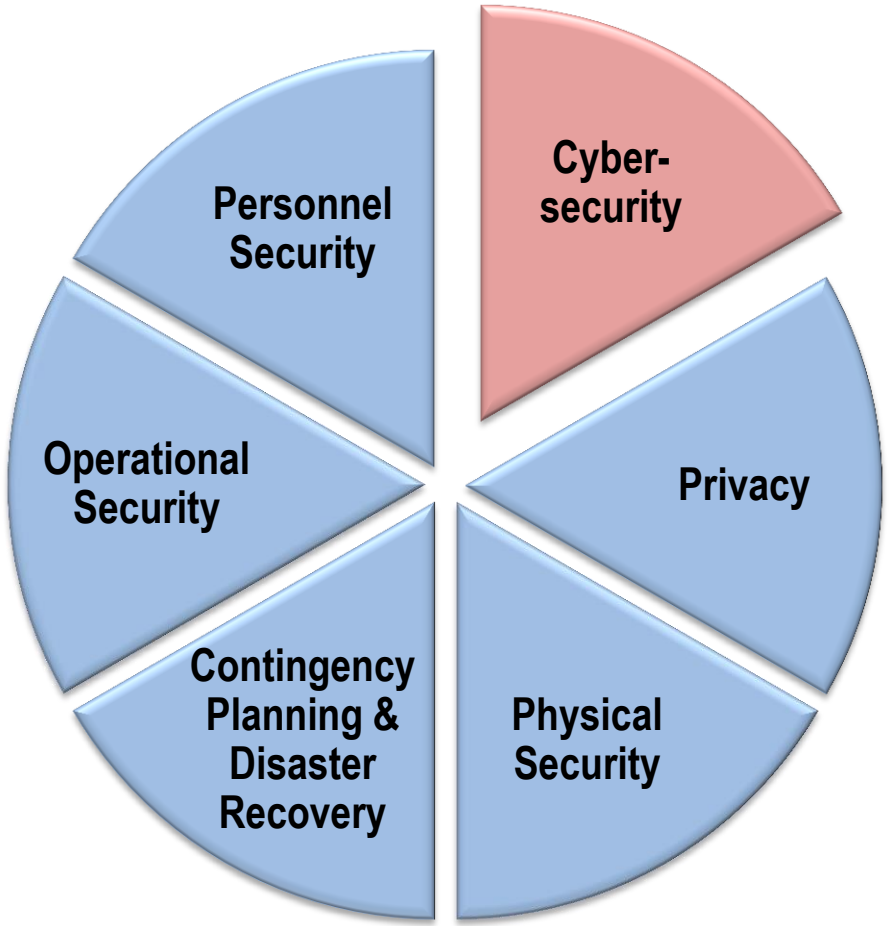
Partnership Model

- Federal, State, Industry
- Managed by NIST at Federal level
- Well aligned with state and local economic development strategies

MEP Strategy: Global Competitiveness and Growth

Provide direct, hands-on technical and business assistance as *trusted advisors* to domestic manufacturers to help them compete and grow

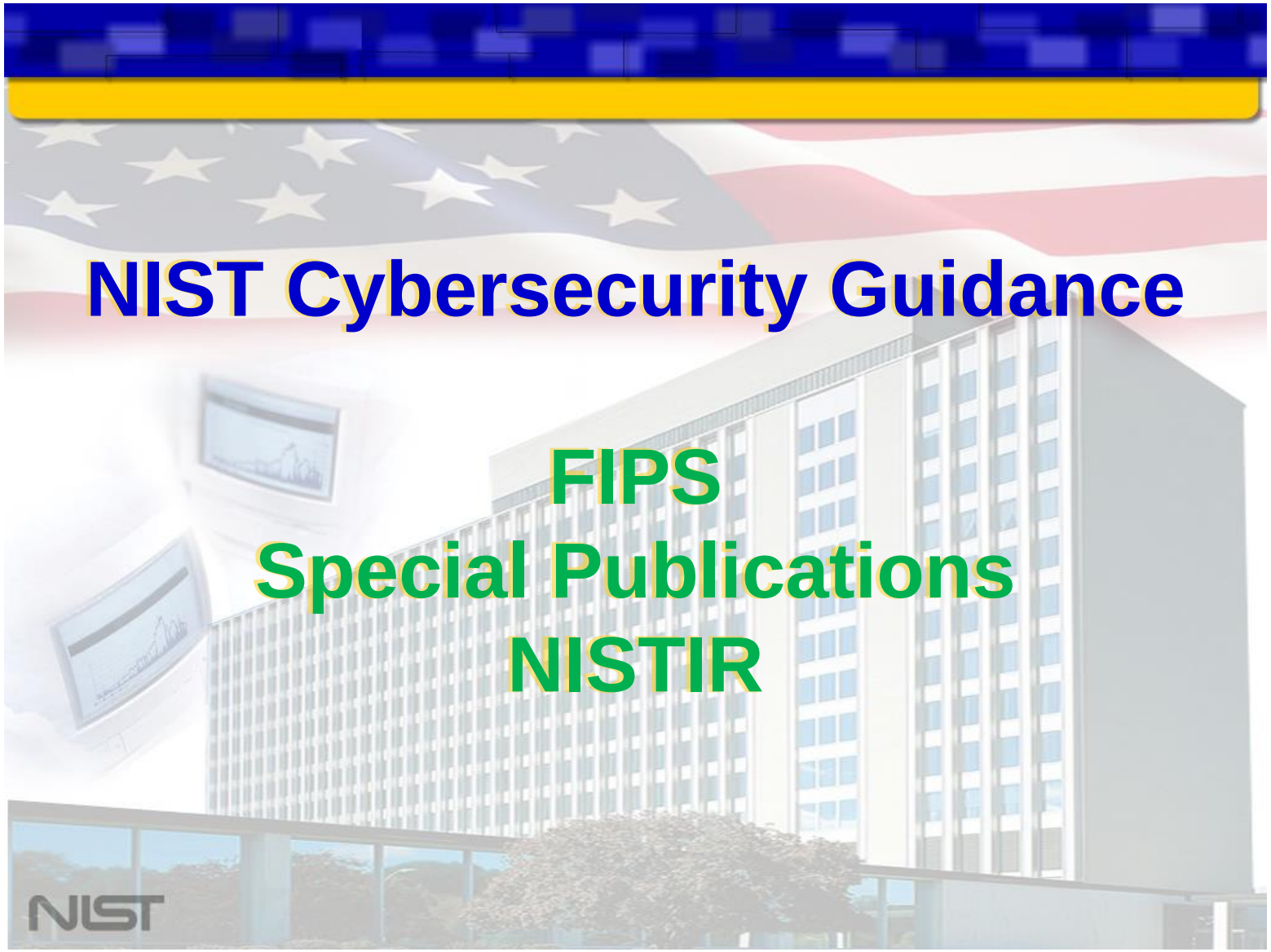
What is Information Security?



Our appetite for *advanced technology* is rapidly exceeding our ability to protect it.

We are vulnerable because our information technology is fragile and susceptible to a wide range of threats including:

- natural disasters.
- structural failures.
- cyber attacks.
- human errors.



- NIST is a non-regulatory agency of the U.S. Department of Commerce.
- Serving as U.S. National Measurement Institute, NIST operates Laboratory programs that support U.S. innovation and standards development.
- NIST does not regulate U.S. cybersecurity – rather, NIST provides neutral technical expertise, guidance, and reference materials that underlie regulations and requirements of other government agencies and industry organizations.
- NIST also manages MEP – the nationwide network of MEP Centers that serve as trusted advisors to U.S. manufacturers in every state and Puerto Rico.

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

Controlled Unclassified Information

Supports federal missions and business functions…

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

Nonfederal Organizations

Some Examples

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

Why is this all necessary?

- Over 100 different ways of characterizing SBU information.
- No common definition or protocols.
- Information inconsistently marked.
- Common definition and standardize processes and procedures.

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

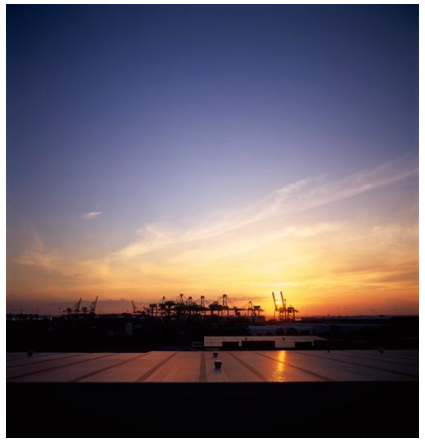
Category-Subcategory:	**Proprietary Business Information-Manufacturer**
Category Description:	Material and information relating to, or associated with, a company's products, business, or activities, including but not limited to financial information; data or statements; trade secrets; product research 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

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.

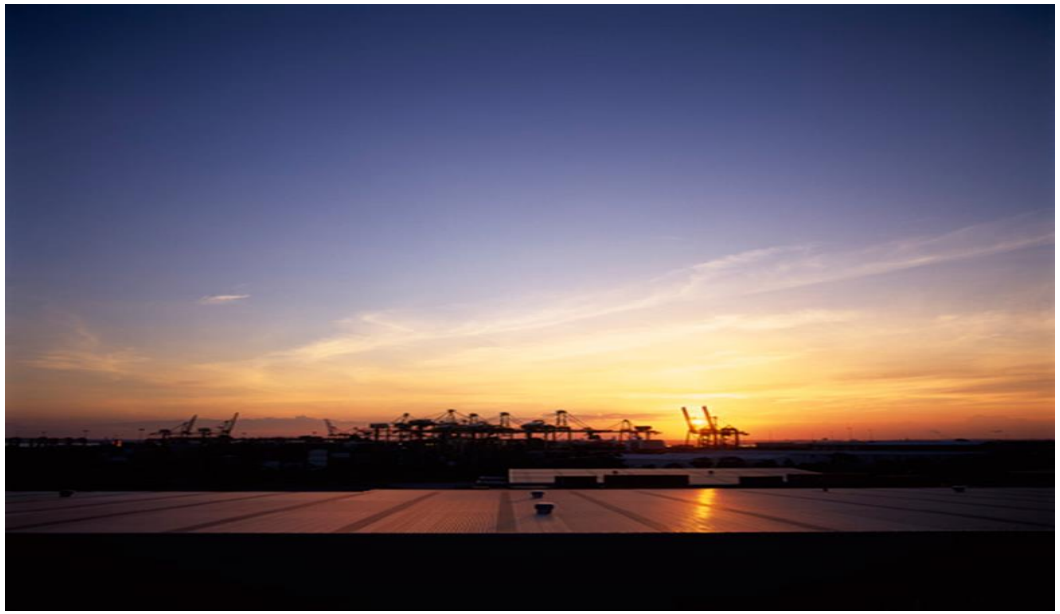
Security Requirements

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

Awareness and Training Example

Basic Security Requirements:

3.2.1 Ensure that managers, systems administrators, and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those organizational information systems.

3.2.2 Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

Derived Security Requirements:

3.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat.

Security Requirement

Awareness and Training Example 3.2.2

Basic Security Requirements:

3.2.2 Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

Meeting the Requirement:

- Basic security awareness training to new employees.
- Security awareness training to users when information system changes.
- Annual security awareness refresher training.

Security Requirement

Awareness and Training Example 3.2.2

Basic Security Requirements:

3.2.2 Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

Meeting the Requirement:

- Security awareness and training policy.
- Security awareness training materials.
- Security plan; training records; other relevant documents or records.
- Personnel with responsibilities for security awareness training.

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.

Security Requirement

Access Control Example

Basic Security Requirements:

3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, or devices (including other systems).

3.1.2 Limit system access to the types of transactions and functions that authorized users are permitted to execute.

Derived Security Requirements:

3.1.3 Control the flow of CUI in accordance with approved authorizations.

3.1.4 Separate the duties of individuals to reduce the risk of malevolent activity without collusion.

3.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts.

3.1.6 Use non-privileged accounts or roles when accessing non-security functions.

3.1.7 Prevent non-privileged users from executing privileged functions and audit the execution of such functions.

3.1.8 Limit unsuccessful logon attempts.

Security Requirement

Access Control Example 3.1.8

Derived Security Requirements:

3.1.8 Limit unsuccessful logon attempts.

Meeting the Requirements:

- Limit number of consecutive invalid logon attempts allowed during a time period.
- Account lockout time period automatically enforced by the information system when max number of unsuccessful logon attempts is exceeded.
- Locks the account/node until released by an administrator.
- Delays next logon prompt according to the organization-defined delay algorithm.
- Access control policy and procedures addressing unsuccessful logon attempts.
- Personnel with information security responsibilities; system developers; system/network administrators

Security Requirement

Access Control Example 3.1.8

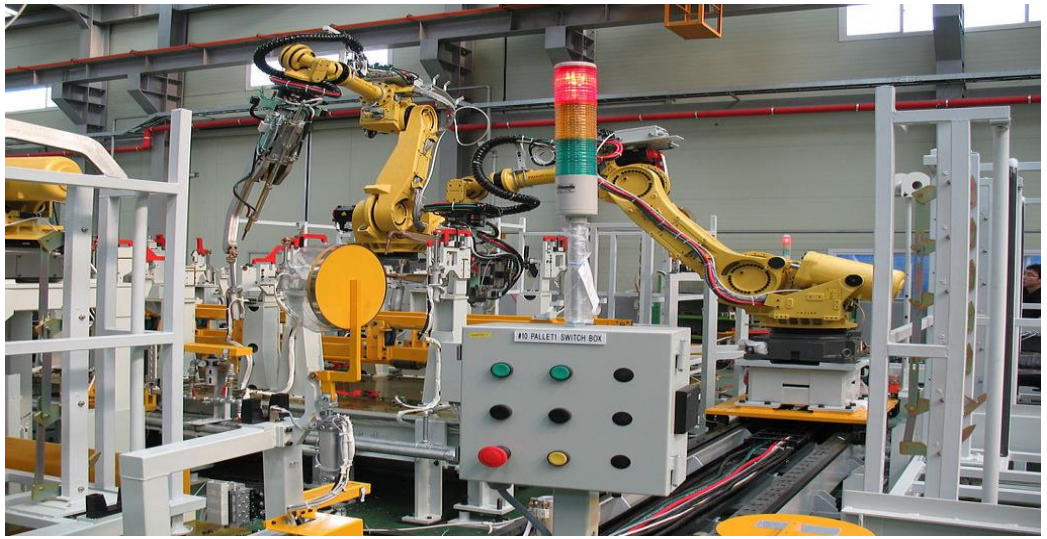
Derived Security Requirements:

3.1.8 Limit unsuccessful logon attempts.

Meeting the Requirements:

- Access control policy and procedures addressing unsuccessful logon attempts.
- Personnel with information security responsibilities; system developers; system/network administrators

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 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.

Contact Info:

Pat Toth
NIST MEP
ptoth@nist.gov
301 975-5140

or

David Stieren
NIST MEP
david.stieren@nist.gov
301-975-3197