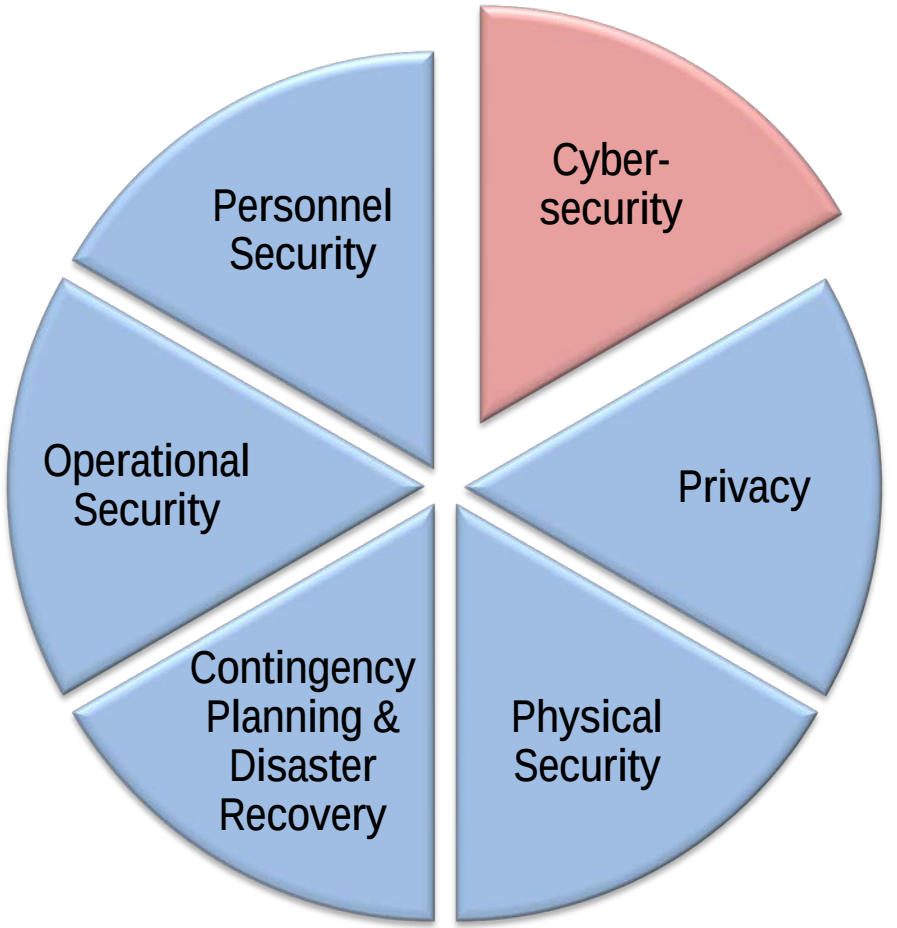
Cybersecurity Risk Management

NIST Guidance
DFARS Requirements
MEP Assistance

David Stieren
Division Chief, Programs and Partnerships
National Institute of Standards and Technology (NIST)
Manufacturing Extension Partnership (MEP)

November 2017

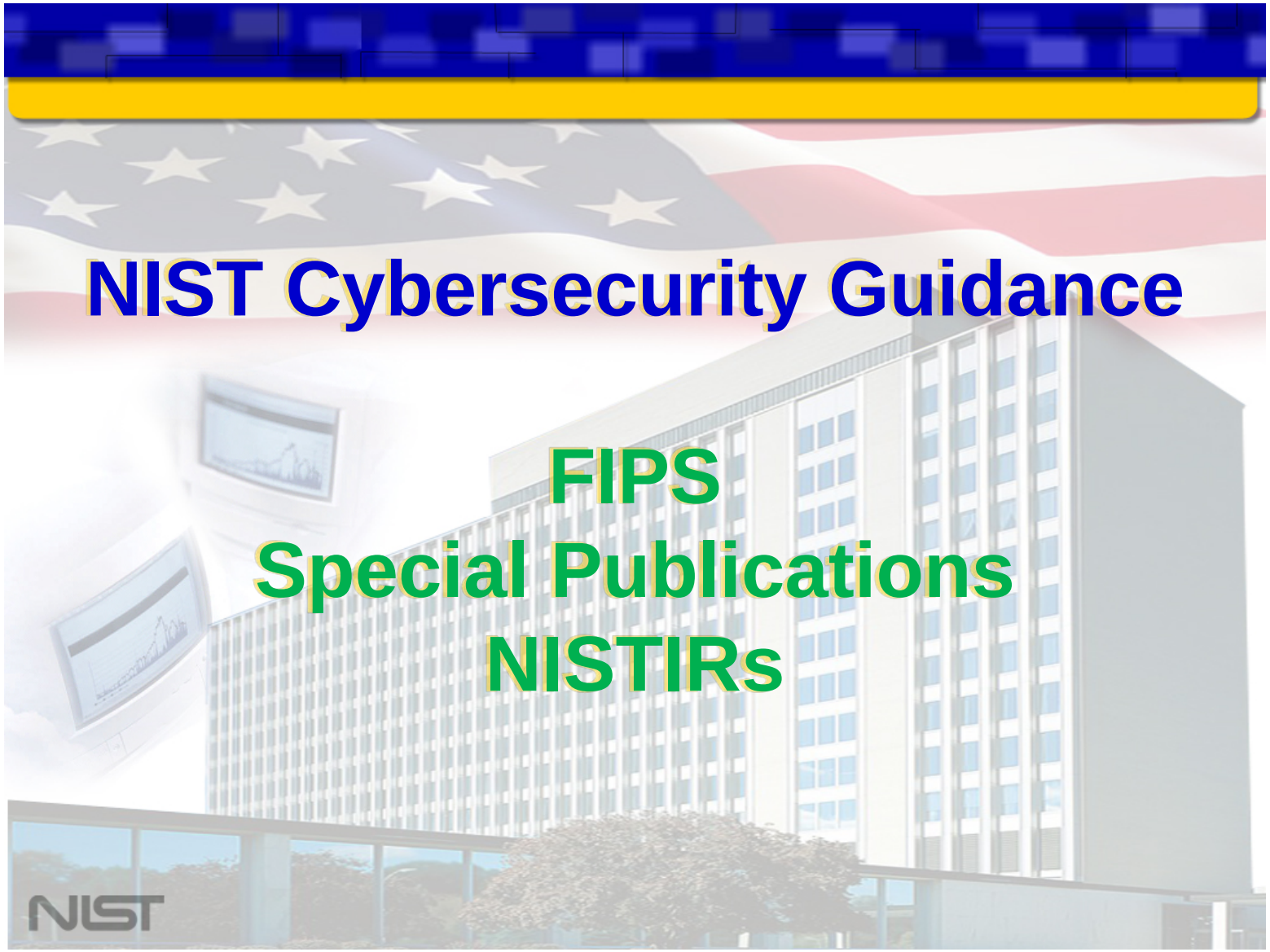
What is Information Security?



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.
- NIST serves as the U.S. National Measurement Institute
  - Operate Laboratory programs that support U.S. innovation, standards development.
    - Focus on metrology and standards
  - Manage the National Network of MEP Centers that provide technical assistance as trusted advisors to U.S. manufacturers in every state and Puerto Rico.
- IMPORTANT:

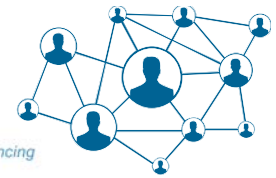
  NIST *does not regulate U.S. cybersecurity* – rather, NIST provides neutral technical expertise, guidance, and reference materials that underlie regulations and requirements of other government agencies and industry organizations.

MEP Summary

MISSION

To strengthen and empower U.S. manufacturers

MEP National Network™
The Go-To Experts for Advancing U.S. Manufacturing



- 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

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

MEP Budget & Business Model

$128M 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

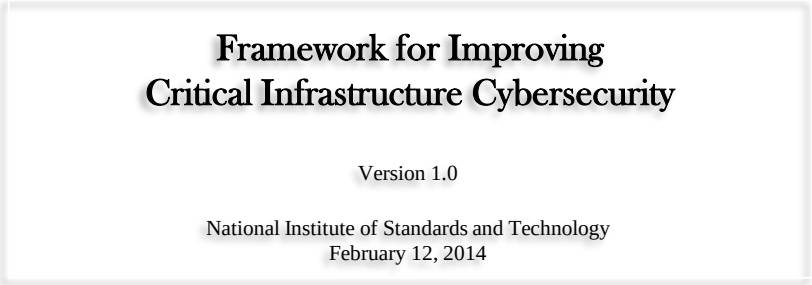
Serve as *trusted advisors* who provide direct, hands-on technical and business assistance to America's manufacturers, striving to be the go-to resource to ensure U.S. manufacturing is resilient and leads the world in manufacturing innovation

NIST Cybersecurity Framework

Presidential Executive Order 13636

"Improving Critical Infrastructure Security"

February 2013


Framework for Improving
Critical Infrastructure Cybersecurity

Version 1.0

National Institute of Standards and Technology
February 12, 2014

- Established that "[i]t is the Policy of the United States to:
  - enhance security and resilience of Nation's critical infrastructure
  - maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties."
- Called for development of voluntary risk-based Cybersecurity Framework
  - set of industry standards and best practices to help organizations manage cybersecurity risks.

NIST Cybersecurity Framework

- The NIST Cybersecurity Framework, created thru collaboration between govt. & private sector, uses common language to address and manage cybersecurity risk in cost-effective way based on business needs – without placing addl. regulatory requirements on businesses.

FRAMEWORK CORE:

Identify
Protect
Detect
Respond
Recover

DFARS

What is the DFARS cybersecurity requirement?

- Clause 252.204-7012 of the DFARS requires defense contractors and subcontractors to:

1. Provide adequate security to safeguard covered defense information (CDI) that resides on or is transiting through a contractor's internal information system or network
2. Report cyber incidents that affect a covered contractor information system or the CDI residing therein, or that affect the contractor's ability to perform requirements designated as operationally critical support
3. Submit malicious software discovered and isolated in connection with a reported cyber incident to the DOD Cyber Crime Center
4. If requested, submit media and additional information to support damage assessment
5. Flow down the clause in subcontracts for operationally critical support, or for which subcontract performance will involve CDI

What is "adequate security"?

- DFARS requires that contractors and their subcontractors employ "adequate security"
- This means that protective measures are employed commensurate with consequences and probability of loss, misuse, or unauthorized access to, or modification of information.
- Contractors should implement, at a minimum, the security controls in NIST SP 800-171 rev 1, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations."
- Contractors are obligated to rapidly report (within 72 hours of discovery) any cyber incident that affects the covered contractor's
  - info system, CDI, or the contractor's ability to provide operationally critical support.
  - Reporting obligations also require that contractors isolate and capture, if possible, an image of the malicious software (e.g., worm, virus, etc.) and provide access to covered contractor info systems and other info if requested by DoD.

What is the purpose of DFARS clause 252.204-7012?

- DFARS 252.204-7012 was structured to ensure that
  - controlled unclassified DoD info residing on a contractor's internal info system is safeguarded from cyber incidents,
  - any consequences associated with the loss of this info are assessed and minimized via the cyber incident reporting and damage assessment processes.

- Also provides single DoD-wide approach to safeguarding covered contractor information systems
  - prevent proliferation of multiple/potentially different safeguarding controlled unclassified information clauses, contract language by various entities across DoD.

What does this DFARS cybersecurity requirement mean?

- This requirement is an included clause in defense contracts.
  - By signing a defense contract, the contractor agrees to comply with the contract terms.
  - DFARS 252.204.7012 applies to info systems that process, store, or transmit CUI.
  - CUI is info that law, regulation, or governmentwide policy requires to have safeguarding or disseminating controls, excluding info 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.

- Examples of CUI include: Controlled Technical Information, Export Control Information, and DoD Critical Infrastructure Security Information.

- For additional information visit the National Archives CUI webpage: https://www.archives.gov/cui

What is a "Covered contractor information system"?

- DFARS 252.204-7012(a): "covered contractor information system"
  - "an unclassified info system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense info."
  - A covered contractor info system is specifically an "unclassified" info system.
  - A covered contractor info system requires safeguarding in accordance with 252.204-7012(b) because performance of the contract requires that the system process, store, or transmit CDI.

When is DFARS clause 252.204-7012 required in contracts?

- DFARS clause 252.204-7012 is required in all solicitations and contracts, including solicitations and contracts using Federal Acquisition Regulation (FAR) part 12 procedures for acquisition of commercial items.

- Clause is not required for solicitations and contracts solely for acquisition of COTS items.

- The clause is not required to be applied retroactively, but that does not preclude a contracting officer from modifying an existing contract to add the clause.

When and how should DFARS clause 252.204-7012 flow down to subcontractors?

- DFARS clause 252.204-7012 flows down to subcontractors without alteration, except to ID the parties, when performance will involve operationally critical support or CDI.
- Per 252.204-7012(m)(1), the prime contractor shall determine if info required for subcontractor performance retains its identity as CDI, thus necessitating flow-down of the clause.
- Contractors should consult the appropriate DOD contracting officer if clarification is required.
- DoD emphasis is on deliberate management of info requiring protection.
  - *Prime contractors should minimize the flow down of info requiring protection.*
- Flow down is a requirement of the terms of the contract with the Government, which should be enforced by the prime contractor as a result of compliance with these terms. If a subcontractor does not agree to comply with the terms of DFARS Clause 252.204–7012, then CDI shall not be on that subcontractor's info system.

What do contractors need to do to ensure compliance with DFARS and when does this apply?

- Defense contractors are required by DFARS to provide *adequate security* on all covered contractor info systems.

- To provide adequate security, defense contractors must implement, at a minimum, the following information security protections:
  - NIST SP 800-171, as soon as practical, but *not later than December 31, 2017*.

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.
- DFARS clause 252.204.7012 requires compliance to NIST Special Publication 800-171

Nonfederal Organizations

Some Examples

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

Controlled Unclassified Information

Supports federal missions and business functions…

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

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

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.

3-Step Process to Complying with DFARS Cybersecurity Requirements

- STEP 1: Develop System Security Plan (SSP) describing
  - the system boundary;
  - the operational environment;
  - how the security requirements are implemented; and
  - the relationships with or connections to other systems
  - can be where Incident Response Plan is provided
- STEP 2: Conduct Assessment, Produce Security Assessment Report
  - conducted against security requirements in NIST SP 800-171
- STEP 3: Produce a Plan of Action with Milestones (POAM)
  - should describe how any unimplemented security requirements will be met and how any planned improvements will be implemented
  - should include detailed milestones used to measure progress

IMPORTANT: Things to Remember Regarding Compliance with DFARS Cybersecurity Requirements

- Compliance occurs upon approval of the SSP, Report of SP 800-171 Assessment, and POAM
  - Approval of these items comes from the appropriate DOD Contracting Officer, or Prime Contractor – depending upon where a particular manufacturer falls within the supply chain
- A contractor's signature on a contract indicates that DFARS cybersecurity requirements have been met
  - There is no 3rd party certification required, nor any requirement for 3rd party assessment
  - No pre-determined audit processes are planned, but audits may occur as warranted

DOD Cybersecurity FAQs from DOD Procurement Toolbox:
http://dodprocurementtoolbox.com/faqs/cybersecurity/frequently-asked-questions-faqs-dated-jan-27-2017-implementation-of-dfars-case-2013

What is NIST SP 800-171 and how does a manufacturer implement it?

- NIST Special Publication (SP) 800-171 developed by NIST to further its statutory responsibilities under Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3541 et seq., Public Law (P.L.) 113-283.
- NIST SP 800-171 provides federal agencies with recommended requirements for protecting the confidentiality of controlled unclassified information (CUI)
- NIST SP 800-171 requirements apply to all components of nonfederal info systems and organizations that process, store, or transmit CUI, or provide security protection for such components.
- CUI requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations. This includes DOD and is resident within DFARS clauses that apply to defense contracts.
- For ease of use, NIST SP 800-171 security requirements are organized into 14 families.

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

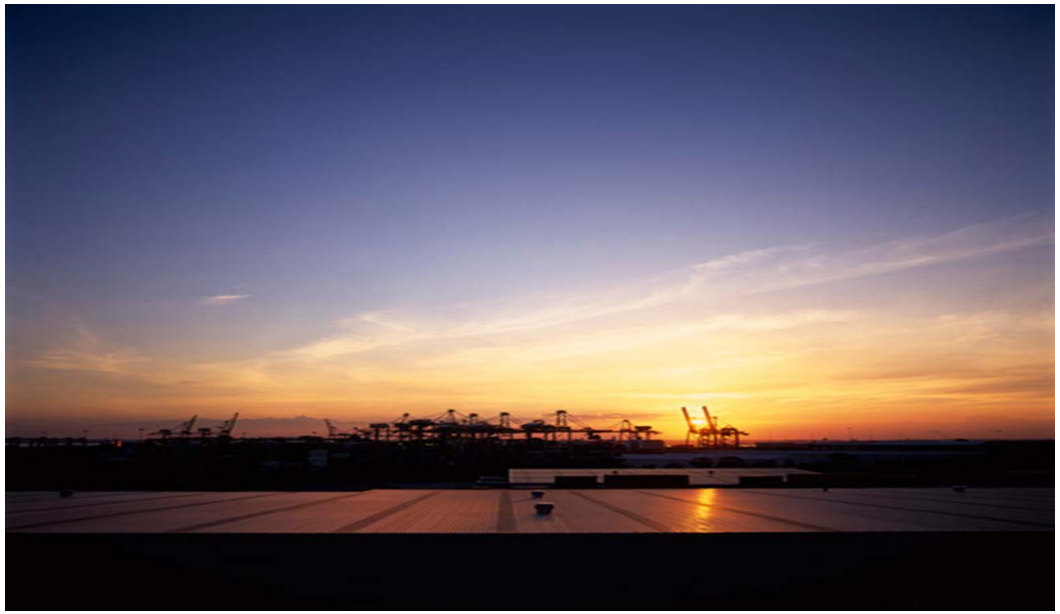
NIST SP 800-171 Security Requirements

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

Meeting SP 800-171

- Emphasis is risk management for a particular operating environment.
- Some security controls may not be applicable to your environment.
- Build off you are currently doing.
- Security controls are intended to be flexible
  - Other ways to meet the requirements.

Meeting SP 800-171

- Cost effective approaches
  - 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.

MEP Activities and Assistance

- MEP Centers offer assistance to small manufacturers implementing 800-171
  - *Training, Web-based resources, FAQs, 3rd Party Service Providers*
  - *Guidance and Tools: basic to advanced*
- ***NIST MEP publish 800-171 Assessment Handbook***
- NIST MEP work with NIST Labs to develop 800-171A, "Building Effective Assessment Plans"
- Closely monitor DFARS developments, maintain close communications with DOD
- Operate national pilot collaboration with PTACs in multiple states to assist small manufacturers with DFARS compliance by end of December 2017
  - *CO, CT, GA, MI, RI, VT, WA initial pilot states, with several other events in other states*
- NIST MEP assist MEP Centers in assuring compliance with DFARS

NIST MEP
800-171 Assessment Handbook

- Step-by-step guide to implementing NIST SP 800-171
- Available in DRAFT format now in internal MEP information repository for MEP Centers to use in providing assistance to U.S. manufacturers
  - Includes Handbook Supplement for MEP Centers to assist manufacturers in compliance with DFARS Cybersecurity Requirements
- Currently also going through NIST editorial review process to be published as an official NIST Handbook
- NIST MEP providing training on usage to MEP Centers

Contact Info:

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

or

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