NIST SP 800-171 Rev1

Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

Path to NIST SP 800-171 - DoD Perspective (1 of 2)

- 2007 – DoD CIO memo to safeguard DoD data in non-DoD systems
  - AT&L tasked to develop DFARS rule/contract clause
- 2007 – Presidential memo - Controlled Unclassified Information (CUI) program
- 2010 – DoD publishes Advance Notice of Proposed Rulemaking for DFARS
  - Public comments complained ‘plain-language’ requirements were vague
  - Restructured requirements to reflect table of selected NIST SP 800-53 controls
- 2010 – President issues E0 13556, NARA designated CUI Executive Agent
- 2011 – DoD publishes *proposed* DFARS rule including table of selected 800-53 controls
- 2012 – Based on comments, DFARS rule re-scoped to protect Unclassified Controlled Technical Information

Path to NIST SP 800-171 – DoD Perspective (2 of 2)

- ***2013 – NARA objects to DFARS in Interagency coordination***
- 2013 – Safeguarding of Unclassified Controlled Technical Information DFARS published
- 2013 – DoD/NARA/NIST begin work on what will become NIST SP 800-171
- 2015 – NIST SP 800-171 published
- 2015 – DFARS rule revised to cite NIST SP 800-171 and apply broadly to 'DoD' CUI
- 2016 – NARA CUI Federal Rule (32 CFR 2002) published

Why NIST SP 800-171?

NARA and NIST objected to DFARS' use of selected subset of 800-53 controls

- Asserted the full moderate impact baseline required for protection of CUI

Concern regarding implementation challenges for non-Federal systems

- 800-53 controls originally developed for Federal systems
  - Some controls/elements should not apply outside the US Government (Federal-centric)
  - Some overly granular when applied to an 'as-built' contractor system
  - Many baseline controls unnecessary (e.g., Availability controls) for protection of CUI

But DFARS' table of 'selected' 800-53 controls also problematic

- Individual controls sometimes include unnecessary elements
- Some controls 'bundle' together disparate requirements unrelated to protecting CUI

Solution - Develop a NIST SP for protection of CUI in nonfederal orgs

- Based on FIPS 200 with control language from 800-53 to meet moderate impact level
- Performance-based to be applicable to existing nonfederal systems
- Eliminate Federal-centric requirements
- Focus on the essentials – providing CUI confidentiality protection

Comparing NIST SP 800-53 to NIST SP 800-171

NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*	**NIST SP 800-171, *Protecting CUI in Nonfederal Information Systems and Organizations, Jun 15***
• Facilitates consistent and repeatable approach for selecting/specifying security controls – Initially focused on systems operated by or for the federal government) – Controls address diverse set of security and privacy requirements across federal government/critical infrastructure	• Developed for use on contractor and other nonfederal information systems to protect CUI. • Tailored to eliminate requirements that are: – Uniquely federal – Not related to CUI (e.g., availability controls) – Expected to be satisfied without specification (i.e., policy and procedural controls)
• "Build It Right" strategy provides flexible yet stable catalog of security controls to meet current information protection needs and the demands of future needs based threats, requirements, and technologies	• Enables contractors to comply using systems and practices they already have in place – Intent is not to require development or acquisition of new systems to process, store, or transmit CUI
• Provides recommended security controls for information systems categorized in accordance with FIPS 199 – Allows organizations to tailor relevant security control baseline to align with their mission/business environment	• Provides pre-tailored and uniform set of requirements for protecting CUI – Allows nonfederal organizations to consistently implement safeguards for the protection of CUI (i.e., one CUI solution for all customers) – Allows contractor to implement alternative, but equally effective, security measures to satisfy every CUI security requirement

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

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

The Big Picture

A three-part plan for the protection of CUI

- Federal CUI regulation (32 CFR Part 2002) establishes required controls and markings for CUI governmentwide.
- NIST Special Publication 800-171 defines security requirements for protecting CUI in nonfederal information systems and organizations.
- Federal Acquisition Regulation (FAR) clause applies the requirements of the federal CUI rule and NIST Special Publication 800-171 to contractors (planned for 2019).

CUI Regulation: *What Does It Say?*

- Codifies that CUI is at least **moderate** for **C**
- Defines “on behalf of an agency”
- Information systems that process, store, or transmit CUI may be *federal* or *nonfederal*
  - When *federal* (including contractors operating *on behalf of*), agency security requirements are applied (i.e., FISMA/RMF)
  - When *nonfederal*, SP 800-171 security requirements are applied

On Behalf of an Agency…

From the CUI Regulation (section 2002.4):

“Occurs when a non-executive branch entity uses or operates an information system or maintains or collects information for the purpose of processing, storing, or transmitting Federal information, and those activities are ***not incidental*** to providing a service or product to the government.”

NIST SP 800-171

Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations.

- **800-171** originally published June 2015
- **800-171 Rev 1** published December 2016
  - New requirement for SSP development
  - Rev 1 **errata** version published 7 June 2018 for consistency with SP 800-171A
    - Discussion Appendix (F) added
    - Minor clarifications made, footnotes added, additions to glossary, etc.

Purpose of SP 800-171

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 of SP 800-171

- 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.

Target Audience

Public and Private Sectors

Individuals with —

- System development life cycle responsibilities
  - Program managers, information owners, mission/business owners
- Acquisition or procurement responsibilities
  - Contracting officers, COTRs
- Information security or risk management responsibilities
  - Authorizing officials, CIOs, CISOs, system owners/security managers
- Security assessment and monitoring responsibilities
  - Auditors, system evaluators, assessors, independent verifiers and validators

Three Primary Assumptions

1. Statutory and regulatory requirements for the protection of CUI are ***consistent***, whether such information resides in federal information systems or nonfederal information systems.
2. Safeguards implemented to protect CUI are ***consistent*** in both federal and nonfederal information systems and organizations.
3. The confidentiality impact value for CUI is no lower than ***moderate*** in accordance with FIPS Publication 199.

Additional 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 controls 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

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.

- 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.

Security Requirements

14 Families

Obtained from FIPS 200 and
NIST Special Publication 800-53

Structure of Security Requirements

Security requirements have a well-defined structure that consists of the following components:

- Basic security requirements from FIPS 200
- Derived security requirements from SP 800-53

Security Requirement

Example from Configuration Management Family

Basic Security Requirements (FIPS 200):

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 (SP 800-53):

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.

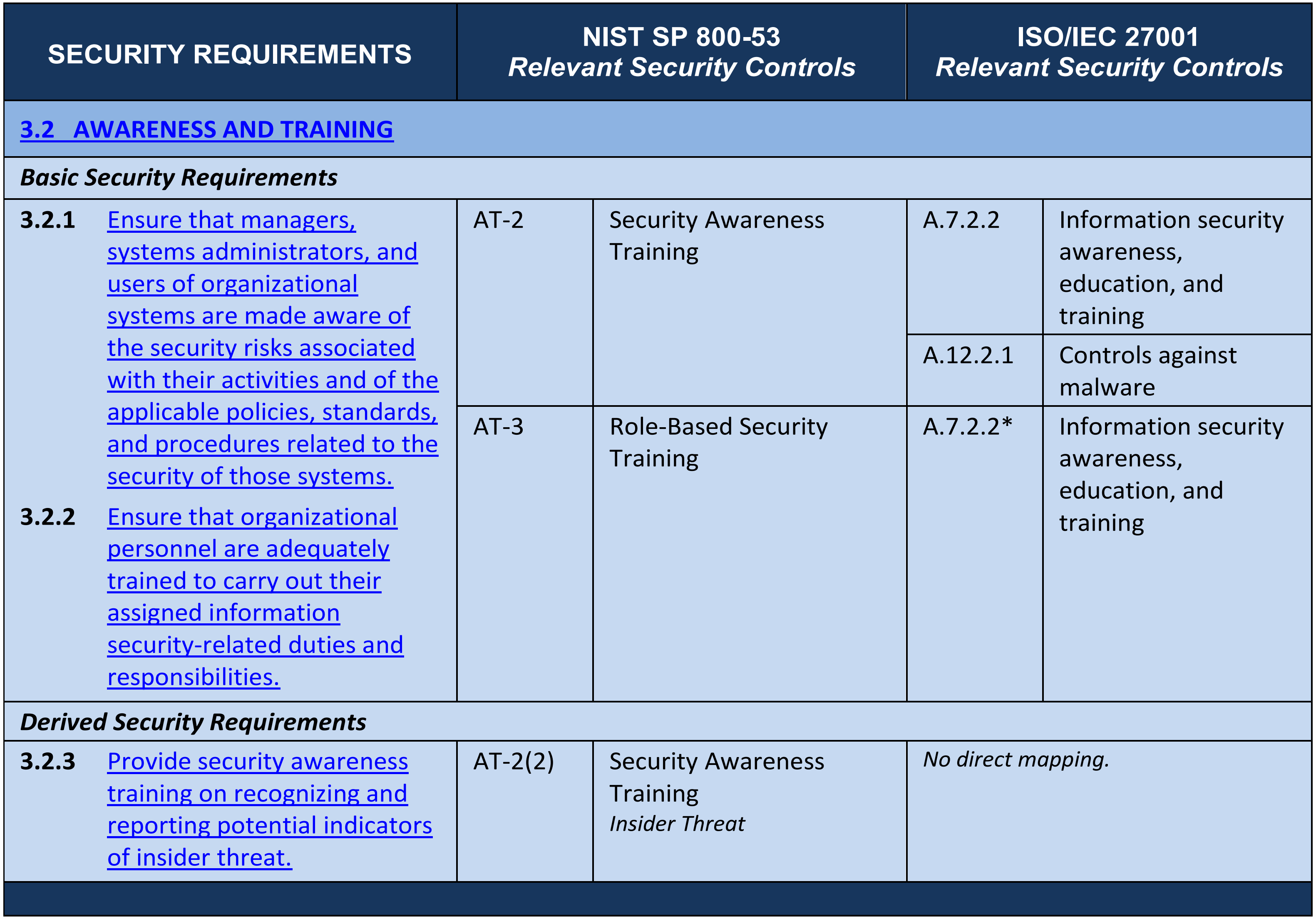
Security Plan

- Describes how SP 800-171 security requirements are met and implemented or future plans
- Describes the system boundary and includes all components that process/store/transmit CUI
- Describes the operational environment
- Describes relationships (dependencies, information exchange, etc.) and/or connections with other systems
- Specifies requirements that are not applicable (e.g., no wireless)
- Submitted to federal organization when requested

Tying it Together:
Two Important Appendices

- Appendix D - Mapping Tables - Maps CUI requirements to ISO 27001 and SP 800-53 Security Controls
- Appendix E - Tailoring Criteria - Tailoring actions applied to moderate security control baseline

SP 800-171 Rev 1 Appendix D Excerpt



SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.2 AWARENESS AND TRAINING				
Basic Security Requirements				
3.2.1 Ensure that managers, systems administrators, and users of organizational 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 systems. **3.2.2** Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.	AT-2	Security Awareness Training	A.7.2.2	Information security awareness, education, and training
			A.12.2.1	Controls against malware
	AT-3	Role-Based Security Training	A.7.2.2*	Information security awareness, education, and training
Derived Security Requirements				
3.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat.	AT-2(2)	Security Awareness Training *Insider Threat*	*No direct mapping.*	

SP 800-171 Rev 1 Appendix E Excerpt

NIST SP 800-53 MODERATE BASELINE SECURITY CONTROLS		TAILORING ACTION
MA-1	System Maintenance Policy and Procedures	NFO
MA-2	Controlled Maintenance	CUI
MA-3	Maintenance Tools	CUI
MA-3(1)	*MAINTENANCE TOOLS | INSPECT TOOLS*	CUI
MA-3(2)	*MAINTENANCE TOOLS | INSPECT MEDIA*	CUI
MA-4	Nonlocal Maintenance	CUI
MA-4(2)	*NONLOCAL MAINTENANCE | DOCUMENT NONLOCAL MAINTENANCE*	NFO
MA-5	Maintenance Personnel	CUI
MA-6	Timely Maintenance	NCO

NFO: Expected to be routinely satisfied; **NCO**: Does not support confidentiality; **CUI**: CUI security requirement; **FED**: Uniquely federal

Security Requirement Discussion*

3.1.4

SECURITY REQUIREMENT

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

DISCUSSION

Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: dividing mission functions and system support functions among different individuals or roles; conducting system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and ensuring that security personnel administering access control functions do not also administer audit functions. Because separation of duty violations can span systems and application domains, organizations consider the entirety of organizational systems and system components when developing policy on separation of duties.

*Originally published in 171A drafts but moved to 171R1 errata dated 7 June 18 as Appendix F

SP 800-171 Supplemental Materials

- https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final
  - SSP Template (doc)
  - POAM Template (doc)
  - Mapping of 171 security requirements to Cybersecurity Framework (xls)

SP 800-171/171A Additional Resources

- NIST’s Manufacturing Extension Partnership’s **Handbook 162**, NIST MEP Cybersecurity Self-Assessment Handbook For Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements
- CUI registry (managed by National Archives and Records Administration - NARA) https://www.archives.gov/cui
- Guidance for Selected Elements of DFARS Clause 252.204-7012: https://www.acq.osd.mil/dpap/policy/policyvault/USA002829-17-DPAP.pdf
- DoD FAQS: http://dodprocurementtoolbox.com/faqs/cybersecurity
- DoD PoC for DFARS Questions: osd.dibcsia@mail.mil

NIST Contact Information

Project Leader and NIST Fellow

Dr. Ron Ross
(301) 975-5390
ron.ross@nist.gov

***Senior Information Security Specialist
And Team Lead***

Victoria Yan Pillitteri
(301) 975-8524
victoria.yan@nist.gov

Senior Information Security Specialist

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

Comments: sec-cert@nist.gov (goes to all of the above)

Web: csrc.nist.gov/sec-cert