Executive Order (EO) on Improving the Nation's Cybersecurity

The Executive Order (EO) on Improving the Nation's Cybersecurity was signed in May and is now in the process of being implemented. The EO is broad ranging in scope, focusing on key areas of vulnerability, including:

- Removing barriers to threat information sharing between government and the private sector
- Modernizing and implementing stronger cybersecurity standards in the federal government
- Improving software supply chain security
- Establishing a cybersecurity safety review board
- Creating a standard playbook for responding to cyber incidents
- Improving detection of cybersecurity incidents on federal government networks
- Improving investigative and remediation capabilities

The principal aim of the EO is to enhance the cybersecurity of government departments and supply chains. However, expect this to have a trickle-down impact on all types of businesses within the private sector, both big and small.

Therefore, small businesses should make themselves aware of the requirements of the EO and determine if they are required to make any changes to remain in compliance, specifically with regards to their vendor relationships.

AN OFFERING IN THE BLUE CYBER SERIES:

NIST SP 800-171 Policies and Procedures An Overview

15 Sep 2021

#17 in the Blue Cyber Education Series

DEFENSE CONTRACT MANAGEMENT AGENCY

NIST SP 800-171 Policies And Procedures

An Overview

Presented By:

Ms. Mia Hazelgrove & Mr. Patrick Wicker

DCMA DIBCAC

December 14th, 2021

NIST 800-171 IN A NUTSHELL

AC	AT	AU	CM	IA	IR	MT	MP	PS	PE	RA	CA	SC	SI
3.1.1	3.2.1	3.3.1	3.4.1	3.5.1	3.6.1	3.7.1	3.8.1	3.9.1	3.10.1	3.11.1	3.12.1	3.13.1	3.14.1
3.1.2	3.2.2	3.3.2	3.4.2	3.5.2	3.6.2	3.7.2	3.8.2	3.9.2	3.10.2	3.11.2	3.12.2	3.13.2	3.14.2
3.1.3	3.2.3	3.3.3	3.4.3	3.5.3	3.6.3	3.7.3	3.8.3		3.10.3	3.11.3	3.12.3	3.13.3	3.14.3
3.1.4		3.3.4	3.4.4	3.5.4		3.7.4	3.8.4		3.10.4		3.12.4	3.13.4	3.14.4
3.1.5		3.3.5	3.4.5	3.5.5		3.7.5	3.8.5		3.10.5			3.13.5	3.14.5
3.1.6		3.3.6	3.4.6	3.5.6		3.7.6	3.8.6		3.10.6			3.13.6	3.14.6
3.1.7		3.3.7	3.4.7	3.5.7			3.8.7					3.13.7	3.14.7
3.1.8		3.3.8	3.4.8	3.5.8			3.8.8					3.13.8	
3.1.9		3.3.9	3.4.9	3.5.9			3.8.9					3.13.9	
3.1.10				3.5.10								3.13.10	
3.1.11				3.5.11								3.13.11	
3.1.12												3.13.12	
3.1.13												3.13.13	
3.1.14												3.13.14	
3.1.15												3.13.15	
3.1.16												3.13.16	
3.1.17													
3.1.18													
3.1.19													
3.1.20													
3.1.21													
3.1.22													

- Administrative (e.g., policies, standards & procedures)
- Technical Configurations (e.g., security settings)
- Software Solution
- Hardware Solution
- Software or Hardware Solution
- Assigned Tasks To Cybersecurity Personnel
- Assigned Tasks To IT Personnel
- Assigned Tasks To Application/ Asset/Process Owner
- Configuration or Software Solution
- Configuration or Software or Hardware or Outsourced Solution

NIST SP 800-171 Policies and Procedures

The Policies and Procedures which you will write for the implementation of NIST SP 800-171 will depend on the data, data flows and Information System architecture of your business.

- In other words, you must do this **SCOPING** work first
- See the Blue Cyber Presentation “Getting Started with NIST SP 800-171”
    - https://www.safcn.af.mil/CISO/Small-Business-Cybersecurity-Information/

Scoping

- It starts with a System Security Plan (SSP) rule #1
  - NIST SP 800-18 is a good reference
  - NIST SP 800-171 (3.12)
- What is " in scope"? See rule #1
  - Enterprise boundary (logical/physical/cloud/ etc..) (3.1, 3.4, 3.5, 3.6, 3.11, 3.13, 3.14)
  - Wireless/mobile/cloud? (3.1, 3.3, 3.4, 3.5, 3.7, 3.9, 3.10, 3.11, 3.13, 3.14)
    - CAAS/virtual enterprise/ etc…
  - Standalone systems (does it process, transmit, or store CUI?)
    - enduring exception?
  - Know what is in the enterprise
    - HW/SW/FW etc… (3.4, 3.5, 3.6, 3.7, 3.11, 3.13, 3.14)
    - Not Applicable? Temporary Deficiency?

Sources that drive the need for policy

Top-down

- Legal
- Regulatory
- Business/Financial
- Executive
- Administrative

Bottom-up

- NIST SP 800-171

Policy Types:

Administrative
Technical
Physical

Controls:

Administrative
Technical
Physical

DFARS 252.204-7012 (Policy inferences)

- Implement security requirements identified in NIST SP 800-171
  - 3.12.4 – “Develop, document and periodically update system security plans…”
- Rapidly (within 72 hours) report cyber incidents
  - 3.6.1 – “Establish an operational incident response handling capability…”
- Submit malicious software to DC3 in accordance with instructions provided by DC3 or the Contracting Officer
- Preserve/protect affected media for 90 days
  - 3.3.1 – “Create and retain system audit logs and records to the extent needed…”
- Flow down DFARS clause requirements to subcontractors

Elements of a Good Policy

Purpose:

The purpose of the policy should be stated clearly and in plain language. If a policy is not written in plain language, employees may not understand it. If an employee can not understand a policy, they may not follow it. If the policy is long-winded or addresses many different topics, then the policy has been diluted and the message trying to be conveyed will lose its meaning. A policy that is short and clear is easily memorable by an employee.

Scope:

The scope of a policy is used to restrict the rules defined by the policy to a specific application or set of circumstances. A well-defined scope will identify what the policy is applied against. Additionally, the scope will identify the intended audience of the policy. A policy should be broad enough that it does not need to change frequently.

Elements of a Good Policy (Cont.)

Roles and Responsibilities:

- Assignment of the activities covered by the policy are defined (responsibilities, authority, ownership, i.e. RACI)
- Separates policy ownership from policy execution
- Establishes or directs establishment of procedures to carry out and meet the intent of the policy

References:

- Regulatory
- Statutory
- Guides
- Standards

Elements of a Good Policy (Cont.)

Leadership Buy-in:

- Leadership should endorse the policy
- Leadership should ensure the policy is available to employees and disseminated appropriately.
- Leadership should appoint a champion to the policy
- Leadership should ensure the policy is reviewed and updated periodically

Defines the Objectives:

- What are you trying to achieve?
- What is the desired outcome?
- Is there a specific target?

Elements of Complete Procedures

Procedures are implanted to enact governance to ensure the objectives of policy are met. Procedures should be:

- Documented
- Repeatable
- Detailed to a sufficient level that minimizes variation
- Specific to activities required to carry out the tasks
- Reviewed and updated periodically

Why Policies and Procedures?

NIST SP 800-171, Appendix E:

APPENDIX E

TAILORING CRITERIA

LISTING OF MODERATE SECURITY CONTROL BASELINE AND TAILORING ACTIONS

This appendix provides a list of the security controls in the [SP 800-53][36] moderate baseline, one of the sources along with [FIPS 200], used to develop the CUI security requirements described in Chapter Three. Tables E-1 through E-17 contain the specific tailoring actions that have been carried out on the controls in accordance with the tailoring criteria established by NIST and NARA. The tailoring actions facilitated the development of the CUI derived security requirements which supplement the basic security requirements.[37] There are three primary criteria for eliminating a security control or control enhancement from the moderate baseline including—

- The control or control enhancement is uniquely federal (i.e., primarily the responsibility of the federal government);
- The control or control enhancement is not directly related to protecting the confidentiality of CUI;[38] or
- The control or control enhancement is expected to be routinely satisfied by nonfederal organizations without specification.[39]

The following symbols in Table E are used in Tables E-1 through E-17 to specify the tailoring actions taken or when no tailoring actions were required.

TABLE E-1: TAILORING ACTIONS FOR ACCESS CONTROLS

NIST SP 800-53 MODERATE BASELINE SECURITY CONTROLS		TAILORING ACTION
AC-1	Access Control Policy and Procedures	NFO
AC-2	Account Management	CUI
AC-2(1)	*ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT*	NCO
AC-2(2)	*ACCOUNT MANAGEMENT | REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS*	NCO
AC-2(3)	*ACCOUNT MANAGEMENT | DISABLE INACTIVE ACCOUNTS*	NCO
AC-2(4)	*ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS*	NCO

Why Policies and Procedures? (Cont.)

SP 800-53 Rev 5.1 and SP 800-53B Latest Versions

AC-1 POLICY AND PROCEDURES

Family: AC - ACCESS CONTROL

Security Baseline:

Low	Moderate	High
AC-1	AC-1	AC-1

Privacy Baseline: AC-1

Jump To:

All Controls > AC > **AC-1**

Control

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
   1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] access control policy that:
      a). Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      b). Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
   2. Procedures to facilitate the implementation of the access control policy and the associated access controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the access control policy and procedures; and

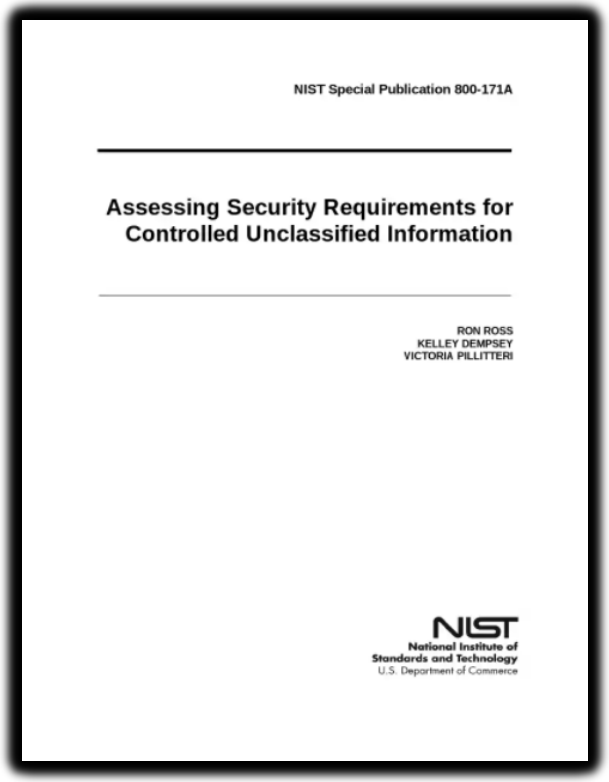
c. Review and update the current access control:
   1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
   2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

Additional Mappings

TABLE D-1: MAPPING ACCESS CONTROL REQUIREMENTS TO CONTROLS

SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.1 ACCESS CONTROL				
Basic Security Requirements				
3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). 3.1.2 Limit system access to the types of transactions and functions that authorized users are permitted to execute.	AC-2	Account Management	A.9.2.1	User registration and de-registration
			A.9.2.2	User access provisioning
			A.9.2.3	Management of privileged access rights
			A.9.2.5	Review of user access rights
			A.9.2.6	Removal or adjustment of access rights
	AC-3	Access Enforcement	A.6.2.2	Teleworking
			A.9.1.2	Access to networks and network services
			A.9.4.1	Information access restriction
			A.9.4.4	Use of privileged utility programs
			A.9.4.5	Access control to program source code
			A.13.1.1	Network controls
			A.14.1.2	Securing application services on public networks

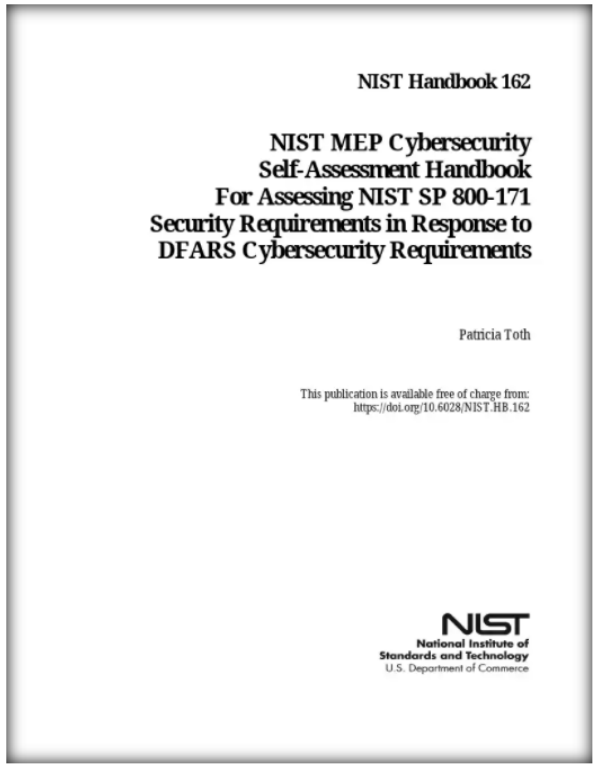
NIST SP 800-171A



- Companion document to NIST SP 800-171r2
- Method for performing DIBCAC CUI assessments
- 320 objectives covering 110 security requirements
- DIBCAC assesses down to the **objective** level
- Many objectives describe potential objects (policies) to examine and elements to be **defined** or **documented**

3.1.3	**SECURITY REQUIREMENT** Control the flow of CUI in accordance with approved authorizations.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.1.3[a] *information flow control policies are defined.*
	3.1.3[b] *methods and enforcement mechanisms for controlling the flow of CUI are defined.*
	3.1.3[c] *designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified.*
	3.1.3[d] *authorizations for controlling the flow of CUI are defined.*
	3.1.3[e] *approved authorizations for controlling the flow of CUI are enforced.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Access control policy; information flow control policies; procedures addressing information flow enforcement; system security plan; system design documentation; system configuration settings and associated documentation; list of information flow authorizations; system baseline configuration; system audit logs and records; other relevant documents or records]. Interview: [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; system developers]. Test: [*SELECT FROM:* Mechanisms implementing information flow enforcement policy].

NIST HB 162



- Assist small manufacturers in preparing for assessment
- Mirrors SP 800-171A
- Self-Assessment Handbook for assessing NIST SP 800-171
- Provides step-by-step guide on assessment methods
  - Examine – Where to Look
  - Interview – Who to Talk To
  - Test – How to Test
- Appendix A – Suggested Plans, Policies, Procedures

NIST HB 162 (Example)

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

Do you have architectural solutions to control the flow of system data?

Yes No Partially Does Not Apply Alternative Approach

Do you document information flow control enforcement by using protected processing level (e.g., defensive architecture) as a basis for flow control decisions?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

The solutions may include firewalls, proxies, encryption, and other security technologies. Information flow control regulates where information can travel within an information system and between information systems (as opposed to who is allowed to access the information) without explicit regard to subsequent accesses to that information.

Examples of flow control restrictions include:

- keeping export-controlled information from being transmitted in the clear to the internet,
- blocking outside traffic that claims to be from within the organization,
- restricting web requests to the internet that are not from the internal web proxy server, and
- limiting information transfers between organizations based on data structures and content.

Transferring information between information systems representing different security domains with different security policies introduces risk that such transfers violate one or more domain security policies. In such situations, information owners/stewards provide guidance at designated policy enforcement points between interconnected systems. The company may consider mandating specific architectural solutions when required to enforce specific security policies. Enforcement includes, for example:

- prohibiting information transfers between interconnected systems (i.e., allowing access only),
- employing hardware mechanisms to enforce one-way information flows, and
- implementing trustworthy regrading mechanisms to reassign security attributes and security label.

Companies commonly employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations (e.g., networks, individuals, and devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Enforcement occurs, for example, in boundary protection devices (e.g., gateways, routers, guards, encrypted tunnels, firewalls) that employ rule sets or establish configuration settings that restrict information system services, provide a packet-filtering capability based on header information, or message filtering capability based on message content (e.g., implementing key word searches or using document characteristics). Companies may also consider the trustworthiness of filtering/inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement.

Where to Look:

- access control policy
- information flow control policies
- procedures addressing information flow enforcement
- information system design documentation
- information system configuration settings and associated documentation
- information system baseline configuration
- list of information flow authorizations information system audit records
- other relevant documents or records

Who to Talk to:

- system/network administrators
- employees with information security responsibilities
- system developers

Perform Test On:

- automated mechanisms implementing information flow enforcement policy

Where to Look:

- access control policy
- information flow control policies
- procedures addressing information flow enforcement
- information system design documentation
- information system configuration settings and associated documentation
- information system baseline configuration
- list of information flow authorizations information system audit records
- other relevant documents or records

Access Control - Policies and Procedures

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

3.1.2[a] - *the types of transactions and functions that authorized users are permitted to execute are defined* (acceptable use policy, remote access policy, privileged user agreement, etc…)

3.1.3 Control the flow of CUI in accordance with approved authorizations

3.1.3[a] *information flow control policies are defined* (email handling policy [safe URL, disallowed attachments, attachment size, phishing reporting], internet use policy [smart filters, blocked categories], removable media policy [restrictions, authorized exceptions, exception process], etc…

3.1.21 Limit use of portable storage devices on external systems

3.1.21[b] - *limits on the use of portable storage devices containing CUI on external systems are defined*

3.1.22 Control CUI posted or processed on publicly accessible systems

3.1.22[c] - *a review process is in place prior to posting of any content to publicly accessible systems*

3.1.22[e] - *mechanisms are in place to remove and address improper posting of CUI* (spillage procedure)

3.1 (Access Control) Policy - Example

3.1.16 Authorize wireless access prior to allowing such connections

- If, the company does NOT allow wireless with documented policy (administrative control)
- Or if the company does NOT allow wireless with additional tool-based policy (technical control)
- Or if the company does NOT allow wireless devices on premise (physical control)
- Then, include those policy languages to the overall policy (SSP)
- Per guidance, it could be considered "satisfied" in the assessment *
  - *verification by assessing entities may want to see the policy
  - *And, or see the technical controls in place

Configuration Management- Policies and Procedures

3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles

3.4.1[b] the baseline configuration includes hardware, software, firmware, and *documentation*.

3.4.5 *Define*, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems

3.4.8 Apply deny-by-exception (blacklisting) *policy* to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) *policy* to allow the execution of authorized software

3.4.9 Control and monitor user-installed software

3.4 (Configuration Management) policy - example

3.4.7 Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services

- 3.4.7[a] essential programs are defined. (documentation: administrative control policy)
- 3.4.7[b] the use of nonessential programs is defined. (documentation: administrative control policy)
- 3.4.7[c] the use of nonessential programs is restricted, disabled, or prevented as defined. (technical control and policy)

Security Assessment - Policies and Procedures

3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application

3.12.1[a] - *the frequency of security control assessments is defined* (information security policy, continuous monitoring policy, etc..)

3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems

3.12.4[g] - *the frequency to update the system security plan is defined* (SSP review frequency, revision history)

System and Information Integrity - Policies and Procedures

3.14.1 Identify, report, and correct system flaws in a timely manner

- 3.14.1[a] - the time within which to identify system flaws is specified (patch management)
- 3.14.1[c] - the time within which to report system flaws is specified (patch management)
- 3.14.1[e] - the time within which to correct system flaws is specified (patch management)

3.14.7 Monitor system security alerts and advisories and take action in response

- 3.14.7[a] - authorized use of the system is defined (acceptable use policy, unacceptable use)

3.14 (System and Information Integrity) example

3.14.1 Identify, report, and correct system flaws in a timely manner

3.14.1[a] the time within which to identify system flaws is specified. (administrative control policy, and may apply to technical control policies)

3.14.1[d] system flaws are reported within the specified time frame. (technical control procedures followed in accordance with administrative and technical control policy)

Common Errors

- Multi-factor authentication not implemented completely
- Not using Federal Information Processing Standards (FIPS) 140-2 VALIDATED cryptography for data in transit and at rest protections
- Poorly written and detailed System Security Plans
- Network Segregation (see Rule #1)
- Configuration management, user installed software lack of policy and enforcement to not allow it

Best Practices

- Know where CUI is processed, transmitted, and stored within your organization
- Maintain a network topology that accompanies your system security plan and describes CUI flow in your organization
- Trace security architecture (policies, processes, appliances, tools) to security requirements addressed in NIST SP 800-171

Questions?

References

- NIST SP 800-171 DoD Assessment Methodology, Version 1.2.1 https://www.acq.osd.mil/asda/dpc/cp/cyber/docs/safeguarding/NIST-SP-800-171-Assessment-Methodology-Version-1.2.1-6.24.2020.pdf
- NIST MEP Cybersecurity Self-Assessment Handbook https://nvlpubs.nist.gov/nistpubs/hb/2017/NIST.HB.162.pdf
- SPRS NIST SP 800-171 Quick Entry Guide https://www.sprs.csd.disa.mil/pdf/NISTSP800-171QuickEntryGuide.pdf
- NIST CUI SSP Template https://csrc.nist.gov/CSRC/media/Publications/sp/800-171/rev-1/final/documents/CUI-SSP-Template-final.docx
- NIST CUI Plan of Action Template https://csrc.nist.gov/CSRC/media//Publications/sp/800-171/rev-1/final/documents/CUI-Plan-of-Action-Template-final.docx
- Supplier Performance Risk System (SPRS) (https://www.sprs.csd.disa.mil/)
- NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171A.pdf