NIST SP 800-171 Automated Mapping Summary

Accurately automate the assessment of NIST SP 800-171 network requirements

NIST SP 800-171 Mapping Document

Nipper automatically analyses NIST SP 800-171 non-compliances it identifies, to reveal the risk to the network if the misconfiguration is exploited, providing an easy way to categorize risks and helping to inform remediation workflows. And for contractors to the Department of Defense, Nipper can also help to assess and evidence SPRS points.

Security Requirement Family	Security Requirement	Nipper	See page
Access Control	3.1.1 Account Management	✓	3
	3.1.8 Unsuccessful Logon Attempts	✓	
	3.1.9 System Use Notification	✓	
	3.1.16 Wireless Access	✓	
Audit Accountability	3.3.1 Event Logging	✓	4
	3.3.2 Audit Record Content	✓	
Configuration Management	3.4.1 Baseline Configuration	✓	4
	3.4.6 Least Functionality	✓	
Identification and Authentication	3.5.1 User Identification, Authentication, and Re-Authentication	✓	5
	3.5.7 Password Management	✓	
System Communication and Protection	3.13.1 Boundary Protection	✓	6
	3.13.6 Network Communications – Deny by Default – Allow by Exception	✓	
System and Information Integrity	3.14.6 System Monitoring	✓	6

Security Requirement Family: Access Control

Security Requirement Family	Security Requirement	Requirement #	Requirement Title	Automated Check
Access Control	Account Management	3.1.1(h)	Require that users log out of the system after [Assignment: organization-defined time period] of expected inactivity or when [Assignment: organization-defined circumstances]	☑
	Unsuccessful Logon Attempts	3.1.8(a)	Enforce a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period]	☑
		3.1.8(b)	Automatically [Selection (one or more): lock the account or node for an [Assignment: organization-defined time period]; lock the account or node until released by an administrator; delay next logon prompt; notify system administrator; take other action] when the maximum number of unsuccessful attempts is exceeded	☑
	System Use Notification	3.1.9	Display a system use notification message with privacy and security notices consistent with applicable CUI rules before granting access to the system	☑
	Wireless Access	3.1.1(d)	Protect wireless access to the system using authentication and encryption	☑

Security Requirement Family: Audit Accountability

Security Requirement Family	Security Requirement	Requirement #	Requirement Title	Automated Check
Audit Accountability	Event Logging	3.3.1(a)	Specify the following event types selected for logging within the system: [Assignment: organization-defined event types]	✓
	Audit Record Content	3.3.2(a)2	Include the following content in audit records: When the event occurred	✓
		3.3.2(a)6	Include the following content in audit records:Identity of the individuals, subjects, objects, or entities associated with the event	✓

Security Requirement Family: Configuration Management

Security Requirement Family	Security Requirement	Requirement #	Requirement Title	Automated Check
Configuration Management	Baseline Configuration	3.4.1(a)	Develop and maintain under configuration control, a current baseline configuration of the system	✓
	Least Functionality	3.4.6(b)	Prohibit or restrict use of the following functions, ports, protocols, connections, and services: [Assignment: organization-defined functions, ports, protocols, connections, and services]	✓
		3.4.6(d)	Disable or remove functions, ports, protocols, connections, and services that are unnecessary or nonsecure	✓

Security Requirement Family: Identification and Authentication

Security Requirement Family	Security Requirement	Requirement #	Requirement Title	Automated Check
Identification and Authentication	User Identification, Authentication, and Re-Authentication	3.5.1(a)	Uniquely identify and authenticate system users, and associate that unique identification with processes acting on behalf of those users	✓
	Password Management	3.5.7(b)	Verify that passwords are not found on the list of commonly used, expected, or compromised passwords when users create or update passwords	✓
		3.5.7(d)	Store passwords in a cryptographically protected form	✓
		3.5.7(e)	Select a new password upon first use after account recovery	✓
		3.5.7(f)	Enforce the following composition and complexity rules for passwords: [Assignment: organization-defined composition and complexity rules]	✓

Security Requirement Family: System Communication and Protection

Security Requirement Family	Security Requirement	Requirement #	Requirement Title	Automated Check
System Communication and Protection	Boundary Protection	3.13.1(a)	Monitor and control communications at external managed interfaces to the system and key internal managed interfaces within the system	☑
	Network Communications – Deny by Default – Allow by Exception	3.13.6	Deny network communications traffic by default and allow network communications traffic by exception	☑

Security Requirement Family: System and Information Integrity

Security Requirement Family	Security Requirement	Requirement #	Requirement Title	Automated Check
System and Information Integrity	System Monitoring	3.14.6) a)1	Monitor the system to detect: Attacks and indicators of potential attack	☑

TITANIA

Get in touch to arrange a demonstration of how to automate the process of assessing network infrastructure and prioritizing remediation based on NIST SP 800-171 risk.

Request a demo

USA
Suite 600,
2451 Crystal Dr, 6th Floor,
Arlington, VA 22202

UK
167-169 Great Portland Street,
London, England,
W1W 5PF