NIST SP 800-53 Mapping Document

Accurately automate the assessment of up to 49 NIST SP 800-53 network controls

NIST SP 800-53 Mapping Document

Titania Nipper is trusted by the US DoD and civilian federal agencies to accurately automate network security and compliance assessments for firewalls, routers and switches against (i) trusted security benchmarks (e.g., DISA STIGs – NDM, RTR and VPN) and (ii) trusted control and risk management frameworks (e.g., NISTSP 800-53).

By virtually modelling device configurations as single entities to consider overlapping rules, Nipper InfraSight achieves an accuracy advantage in detecting configuration drift that is proven to reduce assessment times by up to 80% by not wasting time investigating false positives.

Nipper InfraSight prioritizes vulnerabilities it identifies according to network criticality and provides remediation guidance, improving both the MTTD and MTTR. Additionally, Nipper InfraSight's security and compliance reports provide evidence of both passes and failures.

Nipper OmniSight is capable of assessing the security and compliance posture of up to 250,000 network devices every day. **Through integrations with (i) CMDBs/config repositories and (ii) with SIEMs/GRC platforms, Nipper OmniSight can provide evidence to support:**

1. **Cyber Operational Readiness Assessments (CORA)** enabling teams to detect, respond to, and recover from cyber threats, ensuring compliance with DoD policies while enhancing operational resilience and mission readiness;
2. **Zero Trust** policy assurance, by evidencing (i) networks are segmented with deny all/permit by exception rules and (ii) devices are managed and compliant to IT security policies;
3. **Continuous RMF** and **Continuous Diagnostics and Mitigation (CDM) assurance;** and
4. **Attack Surface Management (ASM)** assurance, by using NIST/MITRE-approved mapping of NIST SP 800-53 controls onto 10 of the 11 MITRE ATT&CK Tactics for Network Infrastructure.

Using DISA STIG Control Correlation Identifiers (CCIs), Nipper InfraSight and Nipper OmniSight automate the accurate assessment of up to 49 NIST SP 800-53 controls and control enhancements across 8 control families.

Access Control

Control Family	Control #	Control	Main Control Supported	Control Enhancement	Low Impact Information Systems	Moderate Impact Information Systems	High Impact Information Systems
Access Control (AC)	AC-2	Account Management		AC-2 (4,7a)	✓	✓	✓
	AC-4	Information Flow Enforcement	AC-4	AC-4 (8,17)		✓	✓
	AC-6	Least Privilege		AC-6 (9)		✓	✓
	AC-7	Unsuccessful Logon Attempts	AC-7 (a)		✓	✓	✓
	AC-8	System Use Notification	AC-8 (a)		✓	✓	✓
	AC-10	Concurrent Session Control	AC-10				✓
	AC-12	Session Termination	AC-12			✓	✓
	AC-17	Remote Access		AC-17 (2)	✓	✓	✓

Audit & Accountability

Control Family	Control #	Control	Main Control Supported	Control Enhancement	Low Impact Information Systems	Moderate Impact Information Systems	High Impact Information Systems
Audit & Accountability (AU)	AU-3	Content Of Audit Records	AU-3	AU-3 (1)	✓	✓	✓
	AU-4	Audit Log Storage Capacity	AU-4	AU-4 (1)	✓	✓	✓
	AU-5	Response To Audit Logging Process Failures		AU-5 (2,4)	✓	✓	✓
	AU-8	Time Stamps	AC-8(b)		✓	✓	✓
	AU-9	Protection Of Audit Information	AU-9		✓	✓	✓
	AU-10	Non-Repudiation	AU-10				✓
	AU-12	Audit Record Generation	AU-12 (a,b,c)		✓	✓	✓

Configuration Management

Control Family	Control #	Control	Main Control Supported	Control Enhancement	Low Impact Information Systems	Moderate Impact Information Systems	High Impact Information Systems
Configuration Management (CM)	CM-5	Access Restrictions For Change		CM-5 (6)	✓	✓	✓
	CM-6	Configuration Settings	CM-6 (b)	CM-6 (1)	✓	✓	✓

Contingency Planning

Control Family	Control #	Control	Main Control Supported	Control Enhancement	Low Impact Information Systems	Moderate Impact Information Systems	High Impact Information Systems
Contingency Planning (CP)	CP-9	System Backup	CP-9 (b)		✓	✓	✓

Identification & Authentication

Control Family	Control #	Control	Main Control Supported	Control Enhancement	Low Impact Information Systems	Moderate Impact Information Systems	High Impact Information Systems
Identification & Authentication (IA)	IA-2	Identification & Authentication (Organizational Users)		IA-2 (8)	✓	✓	✓
	IA-3	Device Identification & Authentication	IA-3	IA-3 (1)		✓	✓
	IA-5	Authenticator Management		IA-5 (1a,b,c) (2,a,c)	✓	✓	✓
	IA-7	Cryptographic Module Authentication	IA-7		✓	✓	✓
	IA-11	Re-Authentication	IA-11		✓	✓	✓

Maintenance

Control Family	Control #	Control	Main Control Supported	Control Enhancement	Low Impact Information Systems	Moderate Impact Information Systems	High Impact Information Systems
Maintenance (MA)	MA-4	Nonlocal Maintenance	MA-4 (e)	MA-4 (6)	✓	✓	✓

System & Communications Protection

Control Family	Control #	Control	Main Control Supported	Control Enhancement	Low Impact Information Systems	Moderate Impact Information Systems	High Impact Information Systems
System & Communications Protection (SC)	SC-5	Denial-Of-Service Protection	SC-5	SC-5 (2)	✓	✓	✓
	SC-7	Boundary Protection	SC-7 (a)	SC-7 (5)	✓	✓	✓
	SC-10	Network Disconnect	SC-10			✓	✓
	SC-13	Cryptographic Protection	SC-13		✓	✓	✓
	SC-17	Public Key Infrastructure Certificates	SC-17			✓	✓
	SC-23	Session Authenticity		SC-23 (3)		✓	✓
	SC-45	System Time Synchronization		SC-45(2)			

System & Information Integrity

Control Family	Control #	Control	Main Control Supported	Control Enhancement	Low Impact Information Systems	Moderate Impact Information Systems	High Impact Information Systems
System & Information Integrity (SI)	SI-11	Error Handling	SI-11(b)			✓	✓

TITANIA

Whether you are looking for an accurate way to assess network-wide compliance with NIST SP 800-53, or need to assure continuous network readiness as a fundamental part of your CORA program, Titania has a solution for you.

Request a demo

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

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