White Paper

Impact of NIST Cybersecurity Framework on Service Providers, Enterprises and NEMs

TABLE OF CONTENTS

1. FRAMEWORK IMPACT

The National Institute of Standards and Technology (NIST) Cybersecurity Framework impacts all public and private organizations that manage critical infrastructures in the United States. The Framework encourages network equipment manufacturers, enterprises, service providers, government agencies and federal integrators to take an active role in risk management with the goal of improving the security posture of critical infrastructures.

Since the Department of Homeland Security (DHS) classifies critical infrastructure as companies in banking & finance, communications, critical manufacturing, defense industrial base, energy, emergency services, food & agriculture, healthcare, IT, utilities, and transportation; the framework impacts most industry sectors. Although compliance with the Framework is optional, legal and accounting firms expect it to be widely adopted by the industry. Executives do not want to be in the position of going to court or being audited and found not in compliance with the framework.

In order to reduce and mitigate the risks associated with their critical infrastructures, organizations need to understand the Framework and assess their critical infrastructures and supply chain. Supply chains start with the **Network Equipment Manufacturers (NEM)** who develop and deliver the network and security devices that manage critical infrastructures. Service providers, enterprises, federal integrators and government agencies need to feel confident that they understand the risks associated with deploying critical infrastructure components that are interconnected and protected by network switches, routers, load balancers, firewalls, Intrusion Prevention Systems and other security tools. The resiliency, stability and vulnerability of critical infrastructure components need to be assessed and tested.

2. RISK ASSESSMENT FOR CRITICAL INFRASTRUCTURES

The Framework approach to risk assessment is based on five core functions that organize cybersecurity activities at their highest level. The five functions are: Identify, Protect, Detect, Respond and Recover. The functions represent the Framework Core. Each function is divided into categories, subcategories and references. The Framework categories and subcategories are groups of activities for a specific function that supports specific outcomes. References are lists of standards, guidelines and practices that are common across critical infrastructure sectors and help implement a subcategory activity. Table 1-1 lists the Framework Core Functions.

Core Function	Identifier	Identifier	Category
Identify	ID	AM	Asset Management
		BE	Business Environment
		GV	Governance
		RA	Risk Assessment
		RM	Risk Management
Protect	PR	AC	Access Control
		AT	Awareness and Training
		DS	Data Security
		IP	Information Protection Processes and Procedures
		MA	Maintenance
		PT	Protective Technology
Detect	DE	AE	Anomolies and Events
		CM	Security Continuous Monitoring
		DP	Detection Process
Respond	RS	RP	Response Planning
		CO	Communications
		AN	Analysis
		MI	Mitigation
		IM	Improvements
Recover	RC	RP	Recovery Planning
		IM	Improvements
		CO	Communications

Table 1-1 Framework Core Functions

2.1. Identify Function

The Identify Function includes the following categories and activities: Asset Management, Business Environment, Governance, Risk Assessment and Risk Management Strategy.

2.1.1. Asset Management

The framework list multiple asset management activities including identifying and taking inventory of physical devices, virtual devices, software platforms and applications. During the asset management identification phase, resources are prioritized based on the classification, criticality and business value of devices, hardware, software and data. Table 1-2 details the asset management activities for the Identify Function.

Subcategory Identifier	Identify Function—Asset Management Category	Framework Test Support
ID.AM-1	Physical devices and systems within the organization are inventoried	Spirent
ID.AM-2	Software platforms and applications within the organization are inventoried	Spirent
ID.AM-3	Organizational communication and data flow are mapped	N/A
ID.AM-4	External information systems are catalogued	Spirent
ID.AM-5	Resources are prioritized based on the classification, criticality and business value	N/A
ID.AM-6	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	N/A

Table 1-2 Asset Management Activities

2.1.2. Business Environment

The activities of the Business Environment category define the organization's mission, objectives and stakeholders. The organization's role in the supply chain and it place in critical infrastructures are identified. Resiliency requirements to support delivery of critical services are established. Table 1-3 details the business environment activities for the Identify Function.

Subcategory Identifier	Identify Function—Business Environment Category	Framework Test Support
ID.BE-1	The organization's role in the supply chain is identified and communicated	N/A
ID.BE-2	The organization's place in critical infrastructure and their industry ecosystem is identified	N/A
ID.BE-3	Priorities for organizational mission, objectives, and activities are established	N/A
ID.BE-4	Dependencies and critical functions for delivery of critical services are established	N/A
ID.BE-5	Resilience requirements to support delivery of critical services are established	Spirent

Table 1-3 Business Environment Activities

2.1.3. Governance

The activities of the Governance category define the organization's security policies, security roles and procedures. Governance revolves around processes used to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements. Table 1-4 details the governance activities for the Identify Function

Subcategory Identifier	Identify Function—Governance Category	Framework Test Support
ID.GV-1	Organizational information security policy is established	Spirent
ID.GV-2	Information security roles & responsibility are coordinated and aligned	Spirent
ID.GV-3	Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	N/A
ID.GV-4	Governance and risk management processes address cybersecurity risks	N/A

Table 1-4 Governance Activities

2.1.4. Risk Assessment & Management

The activities of the Risk Assessment and Risk Management categories were defined to ensure that the organization understands the cybersecurity risks to operations, assets and individuals. Threat and vulnerability information sharing activities are emphasized. Tables 1-5 and Table 1-6 details the risk assessment and management activities for the Identify Function.

Subcategory Identifier	Identify Function—Risk Assessment Category	Framework Test Support
ID.RA-1	Asset vulnerabilities are identified and documented	Spirent
ID.RA-2	Threat and vulnerability information is received from information sharing forums and sources	Spirent
ID.RA-3	Threats, both internal and external are identified and documented	N/A
ID.RA-4	Potential business impacts and likelihoods are analyzed	Spirent
ID.RA-5	Threats, vulnerabilities, likelihoods and impacts are used to determine risk	N/A
ID.RA-6	Risk responses are identified and prioritized	N/A

Table 1-5 Risk Assessment Activities

Subcategory Identifier	Identify Function—Risk Management Category	Framework Test Support
ID.RM-1	Risk management processes are managed and agreed to by organizational stakeholders	N/A
ID.RM-2	Organizational risk tolerance is determined and clearly expressed	N/A
ID.RM-3	The organization's determination of risk tolerance is informed by their role in critical infrastructure and sector specific risk analysis	N/A

Table 1-6 Risk Management Activities

2.2. Protect Function

The Protect Function includes the following categories and activities: Access Control, Awareness & Training, Data Security, Information Protection Processes & Procedures, Maintenance and Protective Technology.

2.2.1. Access Control

The activities of the Access Control category were defined to protect and control access to critical infrastructure assets and information systems. The activities should protect resources from unauthorized access. Table 1-7 details the access control activities for the Protect Function.

Subcategory Identifier	Protect Function—Access Control (AC) Category	Framework Test Support
PR.AC-1	Identities and credentials are managed for authorized devices and users	Spirent
PR.AC-2	Physical access to resources is managed and secured	N/A
PR.AC-3	Remote access is managed	Spirent
PR.AC-4	Access permissions are managed	Spirent
PR.AC-5	Network integrity is protected	Spirent

Table 1-7 Access Control Activities

2.2.2. Awareness & Training

The activities of the Awareness & Training category were designed to ensure the organization's personnel and partners are adequately trained to perform their information security roles and responsibilities. Table 1-8 details the awareness & training activities for the Protect Function.

Subcategory Identifier	Protect Function—Awareness and Training (AT) Category	Framework Test Support
PR.AT-1	All users are informed and trained	N/A
PR.AT-2	Privileged users understand roles & responsibilities	N/A
PR.AT-3	Third-party stakeholders (suppliers, customers, partners) understand roles and responsibilities	N/A
PR.AT-4	Senior executives understand roles and responsibilities	N/A
PR.AT-5	Physical and information security personnel understand roles and responsibilities	N/A

Table 1-8 Awareness & Training Activities

2.2.3. Data Security

The activities of the Data Security category ensure that information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information. Table 1-9 details the data security activities for the Protect Function.

Subcategory Identifier	Protect Function—Data Security (DS) Category	Framework Test Support
PR.DS-1	Data-at-rest is protected	Spirent
PR.DS-2	Data-in-motion is secured	Spirent
PR.DS-3	Assets are formally managed throughout removal, transfers, and disposition	N/A
PR.DS-4	Adequate capacity to ensure availability is maintained	Spirent
PR.DS-5	Protection against data leaks are implemented	Spirent
PR.DS-6	Integrity checking mechanisms are used to verify software, firmware, and information integrity	N/A
PR.DS-7	The development and testing environment(s) are separate from the production environment	Spirent

Table 1-9 Data Security Activities

2.2.4. Information Protection Processes & Procedures

The activities of the Information Protection Processes & Procedures category ensure that security policy, processes, and procedures are maintained and used to manage protection of information systems. Table 1-10 details the information protection processes and procedures activities for the Protect Function.

Subcategory Identifier	Protect Function— Information Protection Processes & Procedures (IP) Category	Framework Test Support
PR.IP-1	A baseline configuration of information technology/operational technology systems is created	N/A
PR.IP-2	A System Development Life Cycle to manage systems is implemented	N/A
PR.IP-3	Configuration change control processes are in place	N/A
PR.IP-4	Backups of information are conducted, maintained, and tested periodically	N/A
PR.IP-5	Policy and regulations regarding the physical operating environment for organizational assets are met	N/A
PR.IP-6	Data is destroyed according to policy	N/A
PR.IP-7	Protection processes are continuously improved	N/A
PR.IP-8	Effectiveness of protection technologies is shared with appropriate parties	N/A
PR.IP-9	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	N/A
PR.IP-10	Response and recovery plans are tested	N/A
PR.IP-11	Cybersecurity is included in human resources practices (e.g., de-provisioning, personnel screening)	N/A
PR.IP-12	A vulnerability management plan is developed and implemented	N/A

Table 1-10 Information Protection Process

2.2.5. Maintenance

The activities of the Maintenance category were developed to ensure that the organization's maintenance and repairs of operational and information system components is performed consistent with policies and procedures. Table 1-11 details the maintenance activities for the Protect Function.

Subcategory Identifier	Protect Function—Maintenance (MA) Category	Framework Test Support
PR.MA-1	Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	N/A
PR.MA-2	Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access and supports availability requirements for important operational and information systems	N/A

Table 1-11 Maintenance Activities

2.2.6. Protective Technology

The activities of the Protective Technology category were developed to ensure that technical security solutions give priority to the security and resilience of systems and assets, consistent with related policies, procedures, and agreements. Table 1-12 details the protective technology activities for the Protect Function.

Subcategory Identifier	Protect Function—Protective Technology (PT) Category	Framework Test Support
PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	N/A
PR.PT-2	Removable media is protected and its use restricted according to policy	N/A
PR.PT-3	Access to systems and assets is controlled, incorporating the principle of least functionality	N/A
PR.PT-4	Communications and control networks are secured	Spirent

Table 1-12 Protective Technology Activities

2.3. Detect Function

The Detect Function includes the following categories and activities: Anomalies and Events, Security Continuous Monitoring, and Detection Processes.

2.3.1. Anomalies and Events

The activities of the Anomalies and Events category were developed to ensure that anomalies are detected in a timely manner and the potential impact of events is understood. Table 1-13 details the anomalies and events activities for the Detect Function.

Subcategory Identifier	Detect Function—Anomalies and Events (AE) Category	Framework Test Support
DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed	N/A
DE.AE-2	Detected events are analyzed to understand attack targets and methods	Spirent
DE.AE-3	Event data are aggregated and correlated from multiple sources and sensors	Spirent
DE.AE-4	Impact of events is determined	N/A
DE.AE-5	Incident alert thresholds are established	Spirent

Table 1-13 Anomalies & Events Activities

2.3.2. Security Continuous Monitoring

The activities of the Security Continuous Monitoring category ensure that information systems and assets are continuously been monitored. The objective is to identify cybersecurity events and verify the effectiveness of protective measures. Table 1-14 details the security continuous monitoring activities for the Detect Function

Subcategory Identifier	Detect Function—Security Continuous Monitoring (CM) Category	Framework Test Support
DE.CM-1	The network is monitored to detect potential cybersecurity events	Spirent
DE.CM-2	The physical environment is monitored to detect potential cybersecurity events	N/A
DE.CM-3	Personnel activity is monitored to detect potential cybersecurity events	N/A
DE.CM-4	Malicious code is detected	Spirent
DE.CM-5	Unauthorized mobile code is detected	Spirent
DE.CM-6	External service provider activity is monitored to detect potential cybersecurity events	N/A
DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed	N/A
DE.CM-8	Vulnerability scans are performed	Spirent

Table 1-14 Security Continuous Monitoring Activities

2.3.3. Detection Processes

The activities of the Detection Process were developed to ensure that processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events. Table 1-15 details the detection processes activities for the Detect Function.

Subcategory Identifier	Detect Function—Detection Processes (DP) Category	Framework Test Support
DE.DP-1	Roles and responsibilities for detection are well defined to ensure accountability	N/A
DE.DP-2	Detection activities comply with all applicable requirements	N/A
DE.DP-3	Detection processes are tested	Spirent
DE.DP-4	Event detection information is communicated to appropriate parties	N/A
DE.DP-5	Detection processes are continuously improved	N/A

Table 1-15 Detection Process Activities

2.4. Respond Function

The Respond Function includes the following categories and activities: Response Planning, Communications, Analysis, Mitigation and Improvements.

2.4.1. Response Planning & Communications

The activities of the Response Planning category ensure that response processes and procedures are maintained and tested to ensure timely response of detected cybersecurity events. The activities of the Communications category ensure that response activities are coordinated with internal and external stakeholders. Table 1-16 details the response planning & communications activities for the Respond Function.

Subcategory Identifier	Respond Function—Response Planning (RP) & Communications (CO)Category	Framework Test Support
RS.RP-1	Response plan is implemented during or after an event	N/A
RS.CO-1	Personnel know their roles and order of operations when a response is needed	Spirent
RS.CO-2	Events are reported consistent with established criteria	N/A
RS.CO-3	Information is shared consistent with response plans	N/A
RS.CO-4	Coordination with stakeholders occurs consistent with response plans, including those related to privacy and civil liberties	N/A
RS.CO-5	Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	N/A

Table 1-16 Response Planning & Communications Activities

2.4.2. Analysis

The activities of the Analysis category were developed to ensure that analysis and forensics functions are conducted. The objective is to ensure adequate response and support recovery activities. Table 1-17 details the analysis activities for the Respond Function

Subcategory Identifier	Respond Function—Analysis (AN) Category	Framework Test Support
RS.AN-1	Notifications from the detection system are investigated	Spirent
RS.AN-2	The impact of the incident is understood	N/A
RS.AN-3	Forensics are performed	N/A
RS.AN-4	Incidents are categorized consistent with response plans	Spirent

Table 1-17 Analysis Activities

2.4.3. Mitigation

The activities of the Mitigation category were developed to prevent expansion of an event, mitigate its effects, and eradicate the incident. Table 1-18 details the mitigation activities for the Respond Function.

Subcategory Identifier	Respond Function—Mitigation (MI) Category	Framework Test Support
RS.MI-1	Incidents are contained	Spirent
RS.MI-2	Incidents are mitigated	N/A
RS.MI-3	Newly identified vulnerabilities are mitigated or documented as accepted risks	Spirent

Table 1-18 Mitigation Activities

2.4.4. Improvements

The activities of the Improvements category ensure that organizational response activities are improved by incorporating lessons learned from current and previous detection & response activities. Table 1-19 details the improvements activities for the Respond Function.

Subcategory Identifier	Respond Function—Improvements (IM) Category	Framework Test Support
RS.IM-1	Response plans incorporate lessons learned	N/A
RS.IM-2	Response strategies are updated	N/A

Table 1-19 Improvements Activities

2.5. Recover Function

The Recover Function includes the following categories and activities: Recovery Planning, Improvements and Communications.

2.5.1. Recovery Planning, Improvements & Communications

The activities of the Recovery Planning category ensure processes and procedures are maintained and tested to ensure timely restoration of systems or assets affected by cybersecurity events. The Improvements category activities were developed to ensure recovery planning and processes are improved by incorporating lessons learned into future activities. The Communications category activities ensure that restoration activities are coordinated with internal and external parties. Table 1-20 details for the Recover Function.

Subcategory Identifier	Recover Function—Recover Planning (RP), Improvements (IM) & Communications (CO) Category	Framework Test Support
RC.RP-1	Recovery plan is executed during or after an event	N/A
RC.IM-1	Recovery plans incorporate lessons learned	N/A
RC.IM-2	Recovery strategies are updated	N/A
RC.CO-1	Public Relations are managed	N/A
RC.CO-2	Reputation after an event is repaired	N/A
RC.CO-3	Recovery activities are communicated to internal stakeholders and executive and management teams	N/A

Table 1-20 Recover Planning, Improvements & Communications Activities

3. CYBERSECURITY TEST TOOLS

Organization entrusted with managing critical infrastructures should leverage the next generation test tools to assess and manage cybersecurity risks. Next generation test tools should empower network equipment manufacturers, enterprises, service providers, government agencies and federal integrators to assess, manage and reduce cybersecurity risks.

3.1. Spirent Solutions

Spirent's next generation test solutions validate that critical infrastructures and their components perform as intended and deliver the protection you expect, using the most intuitive and user friendly interface and test methodologies. Spirent next generation test tools are present in almost every country and every lab providing network equipment manufacturers, service providers, enterprises, government agencies, and federal integrators with the:

- **Ability to test critical infrastructures with realistic traffic that simulates real world applications and security attacks** – with more than 3000 applications including mobile apps.
- **Ability to detect, isolate and prevent**— thousands of known and unknown security attacks and vulnerabilities including zero-day attacks.
- **Ability to operate under attacks, anomalies, variable loads and throughput conditions** — keeping performance high while stopping attacks is critical.
- Avalanche is the leading application and security test tool providing thousands of applications, security attacks, fuzzing attacks and performance testing, enabling users to test network security systems at line rate speeds while simulating daily business traffic to understand the impact of network faults and attacks on critical infrastructures.
- Spirent Studio Security is a testing solution purpose-built for validating security capabilities via fuzz testing, DDOS replication, vulnerability assessment and security capability verification.

SPIRENT

1325 Borregas Avenue
Sunnyvale, CA 94089 USA

AMERICAS 1-800-SPIRENT | +1-818-676-2683 | sales@spirent.com

EUROPE AND THE MIDDLE EAST +44 (0) 1293 767979 | emeainfo@spirent.com

ASIA AND THE PACIFIC +86-10-8518-2539 | salesasia@spirent.com

Rev A. 02/14