NIST Framework for Improving Critical Infrastructure Cybersecurity

NIST Framework for Improving Critical Infrastructure Cybersecurity

- Version 1.1 Issued April 16, 2018
- Based on the Cybersecurity Enhancement Act of 2014 that required NIST to:
  - "Facilitate and support the development of" cybersecurity risk frameworks"
  - Identify "a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risks."

NIST Framework for Improving Critical Infrastructure Cybersecurity

Key Definitions

- Critical Infrastructure: Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters
- DHS defines "Critical Infrastructure Sectors" that perform functions that are supported by the broad category of technology, including information technology (IT), industrial control systems (ICS), cyber-physical systems (CPS), and connected devices more generally, including the Internet of Things (IoT). Sectors are:
  - Chemical
  - Commercial Facilities
  - Communications
  - Critical Manufacturing
  - Dam
  - Defense Industrial Base
  - Emergency Services
  - Energy
  - Financial Services
  - Food and Agriculture
  - Government Facilities
  - Healthcare and Public Health
  - Information Technology
  - Nuclear Reactors, Materials & Waste
  - Transportation Systems
  - Waste and Wastewater Syst

NIST Framework for Improving Critical Infrastructure Cybersecurity

Goal of the NIST Cybersecurity Framework is to provide a common taxonomy and mechanism for organizations to:

- Describe their current cybersecurity posture
- Describe their target state for cybersecurity
- Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process
- Assess progress toward the target state
- Communicate among internal and external stakeholders about cybersecurity risk

NIST Framework for Improving Critical Infrastructure Cybersecurity

NIST Cybersecurity Framework Components:

- Framework Core - a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors.
  - Consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover
  - Identifies underlying key Categories and Subcategories – which are discrete outcomes – for each Function
- Framework Implementation Tiers ("Tiers") - Describe the degree to which an organization's cybersecurity risk management practices exhibit the characteristics defined in the Framework (e.g., risk and threat aware, repeatable, and adaptive). The Tiers characterize an organization's practices over a range, from Partial (Tier 1) to Adaptive (Tier 4)
- Framework Profile ("Profile"): represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories. The Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario

NIST Framework for Improving Critical Infrastructure Cybersecurity

Framework Core Components:

- **Functions** organize basic cybersecurity activities at their highest level. They aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities
- **Categories** are the subdivisions of a Function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities
- **Subcategories** further divide a Category into specific outcomes of technical and/or management activities. They provide a set of results that, while not exhaustive, help support achievement of the outcomes in each Category
- **Informative References** are specific sections of standards, guidelines, and practices common among critical infrastructure sectors that illustrate a method to achieve the outcomes associated with each Subcategory

NIST Framework for Improving Critical Infrastructure Cybersecurity

Framework Core Functions:

- **Identify** – Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities
- **Protect** – Develop and implement appropriate safeguards to ensure delivery of critical services
- **Detect** – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event
- **Respond** – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident
- **Recover** – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident

NIST Framework for Improving Critical Infrastructure Cybersecurity

Framework Core Tiers:

Tier 1: Partial

- *Risk Management Process* – Organizational cybersecurity risk management practices are not formalized, and risk is managed in an *ad hoc* and sometimes reactive manner. Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or business/mission requirements
- *Integrated Risk Management Program* – There is limited awareness of cybersecurity risk at the organizational level. The organization implements cybersecurity risk management on an irregular, case-by-case basis due to varied experience or information gained from outside sources. The organization may not have processes that enable cybersecurity information to be shared within the organization
- *External Participation* – The organization does not understand its role in the larger ecosystem with respect to either its dependencies or dependents. The organization does not collaborate with or receive information (e.g., threat intelligence, best practices, technologies) from other entities (e.g., buyers, suppliers, dependencies, dependents, ISAOs, researchers, governments), nor does it share information. The organization is generally unaware of the cyber supply chain risks of the products and services it provides and that it uses

NIST Framework for Improving Critical Infrastructure Cybersecurity

Framework Core Tiers:

Tier 2: Risk Informed

- *Risk Management Process* – Risk management practices are approved by management but may not be established as organizational-wide policy. Prioritization of cybersecurity activities and protection needs is directly informed by organizational risk objectives, the threat environment, or business/mission requirements
- *Integrated Risk Management Program* – There is an awareness of cybersecurity risk at the organizational level, but an organization-wide approach to managing cybersecurity risk has not been established. Cybersecurity information is shared within the organization on an informal basis. Consideration of cybersecurity in organizational objectives and programs may occur at some but not all levels of the organization. Cyber risk assessment of organizational and external assets occurs, but is not typically repeatable or reoccurring
- *External Participation* – Generally, the organization understands its role in the larger ecosystem with respect to either its own dependencies or dependents, but not both. The organization collaborates with and receives some information from other entities and generates some of its own information, but may not share information with others. Additionally, the organization is aware of the cyber supply chain risks associated with the products and services it provides and uses, but does not act consistently or formally upon those risks

NIST Framework for Improving Critical Infrastructure Cybersecurity

Framework Core Tiers:

Tier 3: Repeatable

- *Risk Management Process* – The organization's risk management practices are formally approved and expressed as policy. Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape
- *Integrated Risk Management Program* – There is an organization-wide approach to manage cybersecurity risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Consistent methods are in place to respond effectively to changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities. The organization consistently and accurately monitors cybersecurity risk of organizational assets. Senior cybersecurity and non-cybersecurity executives communicate regularly regarding cybersecurity risk. Senior executives ensure consideration of cybersecurity through all lines of operation in the organization
- *External Participation* - The organization understands its role, dependencies, and dependents in the larger ecosystem and may contribute to the community's broader understanding of risks. It collaborates with and receives information from other entities regularly that complements internally generated information, and shares information with other entities. The organization is aware of the cyber supply chain risks associated with the products and services it provides and that it uses. Additionally, it usually acts formally upon those risks, including mechanisms such as written agreements to communicate baseline requirements, governance structures (e.g., risk councils), and policy implementation and monitoring

NIST Framework for Improving Critical Infrastructure Cybersecurity

Framework Core Tiers:

Tier 4: Adaptive

- *Risk Management Process* – The organization adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators
- *Integrated Risk Management Program* – There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. The relationship between cybersecurity risk and organizational objectives is clearly understood and considered when making decisions. Senior executives monitor cybersecurity risk in the same context as financial risk and other organizational risks. The organizational budget is based on an understanding of the current and predicted risk environment and risk tolerance. Business units implement executive vision and analyze system-level risks in the context of the organizational risk tolerances. Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities and continuous awareness of activities on their systems and networks. The organization can quickly and efficiently account for changes to business/mission objectives in how risk is approached and communicated
- *External Participation* - The organization understands its role, dependencies, and dependents in the larger ecosystem and contributes to the community's broader understanding of risks. It receives, generates, and reviews prioritized information that informs continuous analysis of its risks as the threat and technology landscapes evolve. The organization shares that information internally and externally with other collaborators. The organization uses real-time or near real-time information to understand and consistently act upon cyber supply chain risks associated with the products and services it provides and that it uses

NIST Framework for Improving Critical Infrastructure Cybersecurity

Framework Profiles:

- Aligns Functions, Categories, and Subcategories with the business requirements, risk tolerance, and resources of the organization
- Establishes a roadmap for reducing cybersecurity risk that is well aligned with organizational and sector goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities
- Can be used to describe the current state or the desired target state of specific cybersecurity activities
  - Current Profile indicates the cybersecurity outcomes that are currently being achieved
  - Target Profile indicates the outcomes needed to achieve the desired cybersecurity risk management goals
  - Comparison of Profiles (e.g., the Current Profile and Target Profile) may reveal gaps to be addressed to meet cybersecurity risk management objectives

NIST Framework for Improving Critical Infrastructure Cybersecurity

Identity Function Categories

- **Asset Management**: The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy
- **Business Environment**: The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions
- **Governance**: The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk
- **Risk Assessment:** The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals
- **Risk Management Strategy**: The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions
- **Supply Chain Risk Management**: The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks

NIST Framework for Improving Critical Infrastructure Cybersecurity

Asset Management Subcategories

- Physical devices and systems within the organization are inventoried
- Software platforms and applications within the organization are inventoried
- Organizational communication and data flows are mapped
- External information systems are catalogued
- Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value
- Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established

NIST Framework for Improving Critical Infrastructure Cybersecurity

Business Environment Subcategories

- The organization's role in the supply chain is identified and communicated
- The organization's place in critical infrastructure and its industry sector is identified and communicated
- Priorities for organizational mission, objectives, and activities are established and communicated
- Dependencies and critical functions for delivery of critical services are established
- Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)

NIST Framework for Improving Critical Infrastructure Cybersecurity

Governance Subcategories

- Organizational cybersecurity policy is established and communicated
- Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners
- Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed
- Governance and risk management processes address cybersecurity risks

NIST Framework for Improving Critical Infrastructure Cybersecurity

Risk Assessment Subcategories

- Asset vulnerabilities are identified and documented
- Cyber threat intelligence is received from information sharing forums and sources
- Threats, both internal and external, are identified and documented
- Potential business impacts and likelihoods are identified
- Threats, vulnerabilities, likelihoods, and impacts are used to determine risk
- Risk responses are identified and prioritized

NIST Framework for Improving Critical Infrastructure Cybersecurity

Risk Management Subcategories

- Risk management processes are established, managed, and agreed to by organizational stakeholders
- Organizational risk tolerance is determined and clearly expressed
- The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis

NIST Framework for Improving Critical Infrastructure Cybersecurity

Supply Chain Management Subcategories

- Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders
- Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process
- Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan
- Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations
- Response and recovery planning and testing are conducted with suppliers and third-party providers

NIST Framework for Improving Critical Infrastructure Cybersecurity

Protect Function Categories

- **Identity Management, Authentication and Access Control**: Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions
- **Awareness and Training**: The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements
- **Data Security**: Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information
- **Information Protection Processes and Procedures**: Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets
- **Maintenance**: Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures
- **Protective Technology**: Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements

NIST Framework for Improving Critical Infrastructure Cybersecurity

Identity Management, Authentication and Access Control Subcategories

- Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes
- Physical access to assets is managed and protected
- Remote access is managed
- Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
- Network integrity is protected (e.g., network segregation, network segmentation)
- Identities are proofed and bound to credentials and asserted in interactions
- Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)

NIST Framework for Improving Critical Infrastructure Cybersecurity

Awareness and Training Subcategories

- All users are informed and trained
- Privileged users understand their roles and responsibilities
- Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities
- Senior executives understand their roles and responsibilities
- Physical and cybersecurity personnel understand their roles and responsibilities

NIST Framework for Improving Critical Infrastructure Cybersecurity

Data Security Subcategories

- Data-at-rest is protected
- Data-in-transit is protected
- Assets are formally managed throughout removal, transfers, and disposition
- Adequate capacity to ensure availability is maintained
- Protections against data leaks are implemented
- Integrity checking mechanisms are used to verify software, firmware, and information integrity
- The development and testing environment(s) are separate from the production environment
- Integrity checking mechanisms are used to verify hardware integrity

NIST Framework for Improving Critical Infrastructure Cybersecurity

Information Protection Processes and Procedures Subcategories

- A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)
- A System Development Life Cycle to manage systems is implemented
- Configuration change control processes are in place
- Backups of information are conducted, maintained, and tested
- Policy and regulations regarding the physical operating environment for organizational assets are met
- Data is destroyed according to policy
- Protection processes are improved
- Effectiveness of protection technologies is shared
- Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed
- Response and recovery plans are tested
- Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)
- A vulnerability management plan is developed and implemented

NIST Framework for Improving Critical Infrastructure Cybersecurity

Maintenance Subcategories

- Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools
- Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access

NIST Framework for Improving Critical Infrastructure Cybersecurity

Protective Technology Subcategories

- Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
- Removable media is protected and its use restricted according to policy
- The principle of least functionality is incorporated by configuring systems to provide only essential capabilities
- Communications and control networks are protected
- Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations

NIST Framework for Improving Critical Infrastructure Cybersecurity

Detect Function Categories

- **Anomalies and Events**: Anomalous activity is detected and the potential impact of events is understood
- **Security Continuous Monitoring**: The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures
- **Detection Processes**: Detection processes and procedures are maintained and tested to ensure awareness of anomalous events

NIST Framework for Improving Critical Infrastructure Cybersecurity

Anomalies and Events Subcategories

- A baseline of network operations and expected data flows for users and systems is established and managed
- Detected events are analyzed to understand attack targets and methods
- Event data are collected and correlated from multiple sources and sensors
- Impact of events is determined
- Incident alert thresholds are established

NIST Framework for Improving Critical Infrastructure Cybersecurity

Security Continuous Monitoring Subcategories

- The network is monitored to detect potential cybersecurity events
- The physical environment is monitored to detect potential cybersecurity events
- Personnel activity is monitored to detect potential cybersecurity events
- Malicious code is detected
- Unauthorized mobile code is detected
- External service provider activity is monitored to detect potential cybersecurity events
- Monitoring for unauthorized personnel, connections, devices, and software is performed
- Vulnerability scans are performed

NIST Framework for Improving Critical Infrastructure Cybersecurity

Detection Processes Subcategories

- Roles and responsibilities for detection are well defined to ensure accountability
- Detection activities comply with all applicable requirements
- Detection processes are tested
- Event detection information is communicated
- Detection processes are continuously improved

NIST Framework for Improving Critical Infrastructure Cybersecurity

Respond Function Categories

- **Analysis**: Analysis is conducted to ensure effective response and support recovery activities
- **Mitigation**: Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident
- **Improvements**: Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities

NIST Framework for Improving Critical Infrastructure Cybersecurity

Analysis Subcategories

- Notifications from detection systems are investigated
- The impact of the incident is understood
- Forensics are performed
- Incidents are categorized consistent with response plans
- Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)

NIST Framework for Improving Critical Infrastructure Cybersecurity

Mitigation Subcategories

- Incidents are contained
- Incidents are mitigated
- Newly identified vulnerabilities are mitigated or documented as accepted risks

Improvements Subcategories

- Response plans incorporate lessons learned
- Response strategies are updated

NIST Framework for Improving Critical Infrastructure Cybersecurity

Recover Function Categories

- **Recovery Planning**: Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents
- **Improvements**: Recovery planning and processes are improved by incorporating lessons learned into future activities
- **Communications**: Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).

NIST Framework for Improving Critical Infrastructure Cybersecurity

Recovery Planning Subcategory

- Recovery plan is executed during or after a cybersecurity incident

Improvements Subcategories

- Recovery plans incorporate lessons learned
- Recovery strategies are updated

Communications Subcategories

- Public relations are managed
- Reputation is repaired after an incident
- Recovery activities are communicated to internal and external stakeholders as well as executive and management teams

NIST Framework for Improving Critical Infrastructure Cybersecurity

How To Use NIST Cybersecurity Framework?

- Compare an organization's current cybersecurity activities with those outlined in the Framework Core
  - Develop a current profile based on the Core Functions, Categories and Subcategories and see where the gaps are against the Core
- Establish or Improve a Cybersecurity Program
  - Develop a current profile, do a risk assessment, create a target profile and determine gaps and implement action plans
- Communicating Cybersecurity Requirements with Stakeholders
  - Provides a connection to Supply Chain Risk Management and thus to the Cybersecurity Executive Order
- Could be used to compare bidders in purchase decisions
- The actual NIST Cybersecurity Framework document does make a case where this framework could be used to determine where a cybersecurity program is going too far with respect to privacy and civil liberty issues