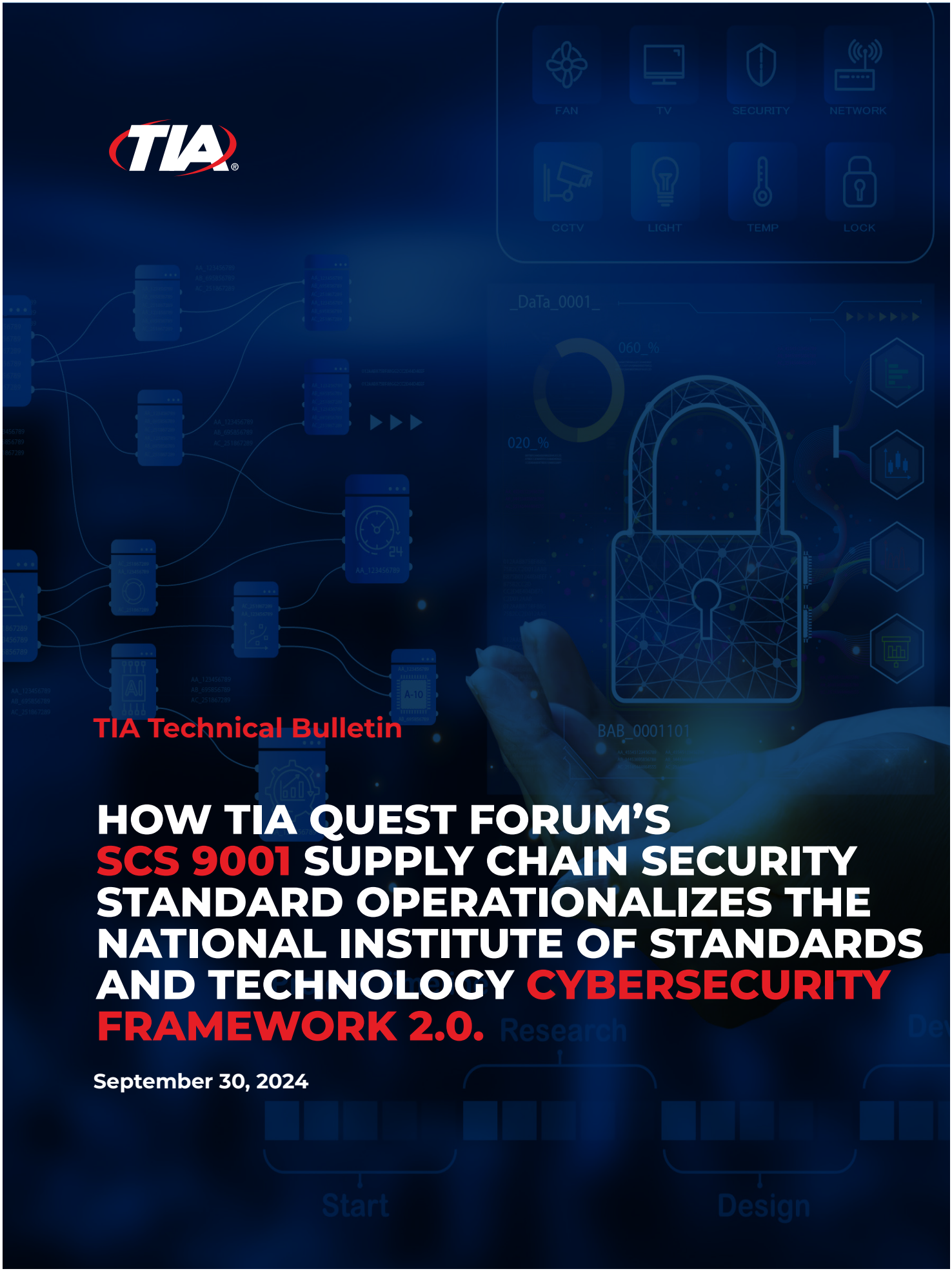


TIA Technical Bulletin

HOW TIA QUEST FORUM'S SCS 9001 SUPPLY CHAIN SECURITY STANDARD OPERATIONALIZES THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY CYBERSECURITY FRAMEWORK 2.0.

September 30, 2024

EXECUTIVE SUMMARY

World governments and their agencies are issuing publications, executive orders and in some cases, legislation intended to drive improvements in network resiliency and reduce impacts of cyber-attacks. Examples include U.S. Executive Order EO14028 and the U.K.'s Telecommunications Security Act of 2021.

As a specific example, the U.S. government has approved the Infrastructure, Investment and Jobs Act (the IIJA). This law appropriates $42.4 billion to the new Broadband Equity, Access, and Deployment (or "BEAD") Program. The BEAD program intends to provide broadband access throughout the entire United Stated and territories. The agency primarily responsible for administering the BEAD Program is the National Telecommunication and Information Agency (NTIA). The BEAD Program requires each state or territory (referred to as an "Eligible Entity") to establish its own program for broadband deployment, subject to NTIA's approval. NTIA will allocate to each Eligible Entity a share of BEAD Program funds based primarily on how many underserved locations are present within the state as compared to the rest of the country.

The logistics of how the program is to operate is described within the publication "Notice of Funding Opportunity (or "NOFO") which was released in May 2022. The NOFO includes a set of attestations that Eligible Entities are to receive from those network operators selected to build the infrastructure (referred to as "Subgrantees").

These attestations are stated as "baseline requirements".

The NOFO requires that at a minimum, prior to allocating funds to a Subgrantee, an Eligible Entity must receive attestation from the Subgrantee that it has a cybersecurity risk management plan which *"reflects the latest version of the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (currently Version 1.1)*[1] *and the standards and controls set forth in Executive Order 14028"*.

Further, the NOFO also requires that prior to allocating funds, an Eligible Entity must receive confirmation from the Subgrantee that it has a supply chain risk management plan *"based upon the key practices discussed in the NIST publication NISTIR 8276 Key Practices in Cyber Supply Chain Risk Management: Observations from Industry and related SCRM guidance within NIST 800-161 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations"*.[2]

This TIA Technical Bulletin provides an overview of NIST's Cybersecurity Framework 2.0 and how the Telecommunications Industry Association (TIA) QuEST Forum's SCS 9001 Supply Chain Security Standard can be used to demonstrate conformance to the requirements and recommendations stated therein.

INTRODUCTION TO THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION (TIA)

The Telecommunications Industry Association (TIA), the trusted industry association for the connected world, represents more than 400 global companies that enable high-speed communications networks and accelerate next-generation ICT innovation. Through leadership in U.S. and international advocacy, technology programs, standards development, and business performance improvement solutions, TIA and its members are accelerating global connectivity across every industry and market. TIA is accredited by the American National Standards Institute (ANSI) and is active in developing and promoting international standards. TIA QuEST Forum brings together companies from around the world who manufacture, deploy and operate cutting edge networks, to develop process-based industry standards and tools to improve business performance and to address the challenges that come with digital transformation, new business models, innovation, and increasing competition.

TIA's QuEST Forum community developed and maintains the ICT industry's most prominent quality standard – TL 9000. As part of our commitment to ensuring global networks are reliable, trusted and secure, TIA QuEST Forum has released the "SCS 9001 Supply Chain Security Management System", a process-based standard focused on supply chain security for the global Information and Communication Technology (ICT) industry.

SCS 9001 is the first comprehensive, measurable, and independently certifiable process-based supply chain security standard for the ICT industry that also benchmarks performance to drive continuous improvement. This standard provides value to network operators of all types and developers and manufacturers of products and services used within those networks.

INTRODUCTION TO NIST'S CYBERSECURITY FRAMEWORK (CSF)

The National Institute of Standards and Technology (NIST) has been operating since 1901 and is part of the U.S. Department of Commerce. The Congress originally created NIST to improve U.S. industrial competitiveness, but the organization has grown significantly and is now influential across many industries and emerging technologies not the least of which are software development, cybersecurity, global communications networks and supply chain risk management.

The NIST Cybersecurity Framework (CSF) was established in response to cybersecurity risks and the need to protect critical infrastructure. The framework's genesis can be traced back to Executive Order 13636, issued on February 12, 2013, which called for the development of a standardized security framework due to the increasing risks to critical infrastructure. The National Institute of Standards and Technology (NIST), known for its non-regulatory role and expertise in standards and best practices, was tasked with creating the framework. The development process was collaborative, involving stakeholders from government, industry, and academia, and utilized a Request for Information (RFI) and Request for Comment (RFC) to gather input. This inclusive approach ensured that the framework would be comprehensive and applicable across various sectors.

The CSF was first released in 2014 and has since undergone updates to address the evolving landscape of cybersecurity threats and technologies. The core of the original framework was organized around five key functions: Identify, Protect, Detect, Respond, and Recover, which provide a high-level taxonomy of cybersecurity outcomes and a strategic view of the lifecycle of managing cybersecurity risk. The CSF is designed to be flexible and adaptable, allowing organizations of different sizes, sectors, and complexities to apply it according to their specific needs and risk profiles.

Applications of the CSF are wide-ranging and serve as a voluntary guide to help organizations manage and reduce cybersecurity risks while protecting their networks and data. The framework is not prescriptive but offers a set of best practices and desired outcomes, enabling organizations to prioritize their efforts effectively. For instance, the CSF has been used to develop community profiles, which are customized implementations of the framework that address the unique needs and risk landscapes of specific communities or sectors.

UPDATES IN NIST CSF VERSION 2.0

In February 2024, NIST released a significant update to the Cybersecurity Framework as CSF 2.0. This update marks the first major revision since the framework's inception in 2014 and aims to address the evolving cybersecurity landscape. The new version expands its applicability beyond critical infrastructure sectors, making it relevant for organizations of all sizes and types.

A notable change in this release is the addition of a sixth function, 'Govern,' which underscores the importance of governance in managing cybersecurity risks. This function complements the existing five functions—Identify, Protect, Detect, Respond, and Recover—by emphasizing the strategic decision-making process at the senior leadership level.

CSF 2.0 also introduces a new category within the Identify function, focusing on continuous improvement and the importance of developing and updating cybersecurity profiles and action plans. This reflects a shift towards a more dynamic approach to cybersecurity, recognizing that the threat environment is constantly changing, and organizations must adapt accordingly.

CSF 2.0 is a response to public comments and a multiyear process of discussions, reflecting the latest cybersecurity challenges and management practices. TIA was an active member of the group that reviewed and provided comments on proposed changes.

The transition from NIST Cybersecurity Framework (CSF) 1.0 to 2.0 represents a significant evolution in the approach to cybersecurity, reflecting the dynamic and increasingly complex digital threat landscape. One of the primary differences is the expanded scope of CSF 2.0, which now extends its applicability beyond the U.S. critical infrastructure to organizations of all sizes and industries worldwide. This global embrace acknowledges the universal nature of cybersecurity threats and the need for a standardized approach to managing them.

Finally, CSF 2.0 enhances guidance and governance with new subcategories that cover risk appetite, tolerance, supply chain and response options.

INTRODUCTION TO TIA SCS 9001

SCS 9001 defines requirements for implementation of a **Supply Chain Security Management System (SCSMS)**. It is a certifiable, process-based global standard with a specific focus on securing **the supply chain** of organizations operating in the Information and Communications Technology (ICT) industry.

As prerequisites in securing its supply chain, an organization must demonstrate that it practices a proper level of cybersecurity to protect its operations, information, development process, and end products. SCS 9001 was developed to provide assurance of the proper operational hygiene of network operators and their suppliers in delivering products and services of inherently higher security.

SCS 9001 was developed to help evaluate and provide higher assurance that organizations:

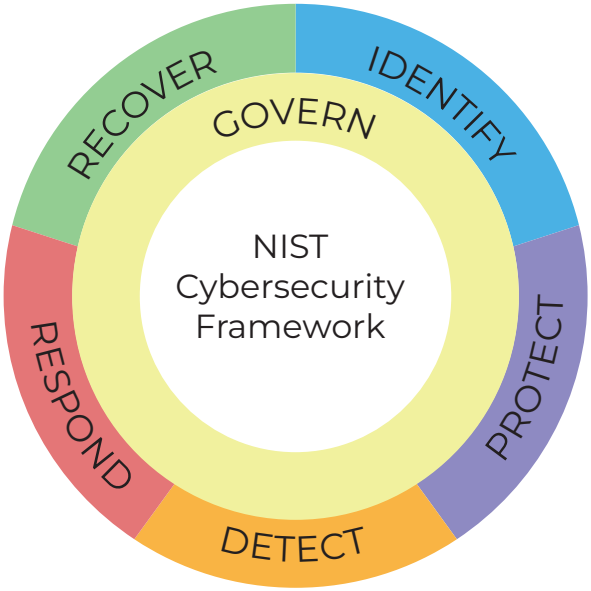
- operate their businesses with integrity, and are transparent and trustworthy,
- conduct all aspects of operations with a high level of security consideration,
- develop products and services with security built in from conception and considered through-out the entire lifecycle,
- can demonstrate effective management of their own suppliers by ensuring the provenance of products and components from approved reputable sources in the final product,
- have made requisite investments to support their products through their entire lifecycle, including the ability to more quickly identify, mitigate and resolve vulnerabilities found post-deployment.

OVERVIEW OF THE NIST CYBER SECURITY FRAMEWORK[3]

The graphic below shows the CSF Functions as a wheel because all of the Functions relate to one another. For example, an organization will categorize assets under IDENTIFY and take steps to secure those assets under PROTECT. Investments in planning and testing in the GOVERN and IDENTIFY Functions will support timely detection of unexpected events in the DETECT Function, as well as enabling incident response and recovery actions for cybersecurity incidents in the RESPOND and RECOVER Functions. GOVERN is in the center of the wheel because it informs how an organization will implement the other five Functions.

An overview of each Function follows:

- **GOVERN (GV):** The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.
- **IDENTIFY (ID):** The organization's current cybersecurity risks are understood.
- **PROTECT (PR):** Safeguards to manage the organization's cybersecurity risks are used.
- **DETECT (DE):** Possible cybersecurity attacks and compromises are found and analyzed.
- **RESPOND (RS):** Actions regarding a detected cybersecurity incident are taken.
- **RECOVER (RC):** Assets and operations affected by a cybersecurity incident are restored.



Graphic 1 – CSF Relation Wheel

Each of the CSF Functions contains a number of related Categories and an Identifier for ease of reference. The table which follows identifies all Functions, the associated Categories within those Functions, and the Category Identifier.

FUNCTION	CATEGORY	CATEGORY IDENTIFIER
Govern (GV)	Organizational Context	GV.OV
	Risk Management Strategy	GV.RM
	Roles, Resposibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identity (ID)	Asset Management	ID.AM
	RIsk Assessment	ID.RA
	Improvement	ID.IM
Potect (PR)	Identity Management, Authetification, and Access Control	PR.AA
	Awereness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

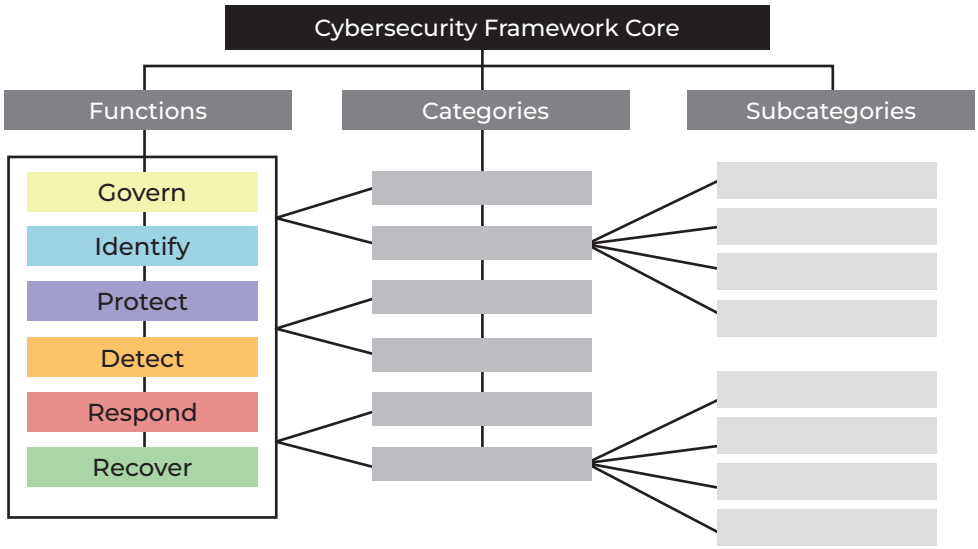
Table 1 – CSF 2.0 Functions, Categories and Category Identifiers

Each Category also includes a number of Subcategories. Subcategories are specific outcomes of technical and management cybersecurity activities that comprise the respective Category.

Organizations can use the CSF to help identify, assess, and manage cybersecurity risk. It is not intended to replace existing processes; it is used to assist organizations with identifying gaps in implemented cybersecurity programs versus the intended end-state. The CSF complements existing cybersecurity practices and serves as the foundation for new cybersecurity programs or improvements to existing practices.

CSF STRUCTURE

The CSF is composed of three components: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles as illustrated in the following graphic:



Graphic 2 - CSF Structure

These components are briefly explained below.

Framework Core: a set of activities with desired outcomes from industry standards, guidelines, and best practices. The Core allows for communication of cybersecurity activities and outcomes within and across organizations.

The Framework Core consists of six Key Functions named Govern, Identify, Protect, Detect, Respond, Recover. These Key Functions provide a high-level view of the lifecycle of an organization's management of cybersecurity risk including the underlying Key Activities to be implemented.

Framework Implementation Tiers: the Tiers provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. Tiers describe the degree to which an organization's cybersecurity risk management practices follow the CSF.

The Tiers are not a maturity model but are intended to demonstrate the advancement of the organization's implementation of the CSF. The Tiers assess criteria of the implemented Risk Management Process, the existence of an Integrated Risk Management Program, and the level of External Participation in which the organization engages.

A brief overview of each Tier follows.

- **Tier 1 – Partial:** cybersecurity risk management practices are not formalized. Risk is managed in an ad hoc manner. There is limited awareness of cybersecurity risk across the organization. The organization has limited understanding of its role in the larger ecosystem with respect to its dependencies and dependents and is generally unaware of the cyber supply chain risks of the products and services it provides and uses.
- **Tier 2 - Risk Informed:** risk management practices are approved by management but may not be established as policy. There is an awareness of cybersecurity risk but an organization-wide approach managing the risk has not been established. Cybersecurity information is shared within the organization on an informal basis. Cyber risk assessment of organizational and external assets occurs but is not typically repeatable. The organization generally understands its role in the larger ecosystem and collaborates with and receives some information from other entities and generates some of its own information but not consistently. Finally, 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 upon those risks.
- **Tier 3 – Repeatable:** the organization's risk management practices are formalized. Organizational cybersecurity practices are regularly updated. There is an organization-wide approach to manage cybersecurity risk through documented policies, processes, and procedures. 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 executives ensure consideration of cybersecurity through all lines of operation in the organization. The organization understands its role, dependencies, and dependents in the larger ecosystem and collaborates 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 and acts upon those risks.
- **Tier 4 – Adaptive:** the organization continuously adapts and improves its cybersecurity practices. There is an organization-wide approach to managing cybersecurity risk. The relationship between cybersecurity risk and organizational objectives is considered when making decisions. Cybersecurity risk is monitored in the same context as financial risk and other organizational risks. Cybersecurity risk management is engrained within the organizational culture. Established procedures enable quick reaction to changing objectives. The organization actively participates in the larger ecosystem of information sharing with collaborators. The organization uses real-time or near real-time information to act upon cyber supply chain risks associated with the products and services it provides and that it uses. Finally, the organization communicates proactively using formal agreements to develop and maintain strong supply chain relationships.
- **Framework Profile:** the Profile can be characterized as the alignment of standards, guidelines, and practices to the Core. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing the Current Profile (the level to which the organization has operationalized the CSF) to the Target Profile (the desired state). Profiles are used to support continuous improvement and to prioritize and measure progress towards the Target Profile with consideration of business needs including cost effectiveness and innovation. Profiles can be used to conduct self-assessments and communicate within an organization or between organizations.

COMPARISON OF THE NIST CSF AND TIA SCS 9001

The CSF is a framework with a purpose of providing guidance on how to manage cybersecurity risks. It DOES NOT prescribe how outcomes should be achieved. The current version of the CSF has added 10 Subcategories in support of supply chain security risk management. These Subcategories represent a limited baseline in consideration of supply chain security risk management. By themselves they are insufficient to implement a comprehensive supply chain security management system.

As a process-based certifiable standard, SCS 9001 is designed to ensure that organizations consistently produce outcomes that meet customer requirements and comply with applicable regulations. Process-based standards are intended to help organizations improve efficiency, achieve operational excellence, and enhance customer satisfaction by adopting a systematic approach to managing and optimizing their processes. They emphasize the importance of understanding customer needs, establishing clear quality and security objectives, and engaging in continuous improvement. By becoming certified, organizations can demonstrate their commitment to quality and security, which can increase trust with customers and stakeholders and create a competitive advantage.

As a process-based standard, SCS 9001 approaches the problem of supply chain security in a more powerful fashion by integrating the controls of other standards within its defined processes. These processes are measured and continuously improved. Publications originally considered and built upon include ISO 27001, ISO 27017, CMMC, ISO 27032, and the NIST CSF, as examples. SCS 9001 has continued to evolve and tracks many other additional publications.[4]

The CSF is organized around its defined Functions and Categories. SCS 9001 conforms to ISO Annex SL. ISO Annex SL, also known as the High-Level Structure (HLS), is a framework that provides a standardized structure for all ISO management system standards. It was introduced to ensure consistency and compatibility between different management system standards, making it easier for organizations to integrate multiple standards within their management systems.

The CSF defines 6 Functions, 22 Categories and 106 Subcategories. The Subcategories are essentially the requirements of CSF. SCS 9001 includes over 800 requirements and 60 controls.

SCS 9001 includes equivalent protections as the CSF cybersecurity Subcategories, but greatly extends the supply chain security requirements as detailed in the section titled “SCS 9001 Supply Chain Security Requirements Extending Beyond CSF Subcategories” further in this Technical Bulletin.

CSF MAPPING TO SCS 9001

The table that follows lists all CSF Functions, Categories and Subcategories mapped to the primary SCS 9001 requirement and/or control that corresponds to each CSF Subcategory.

The color coding of the table maintains that used within the CSF for ease of reference.

Note that there are discontinuities in the sequential number of the Subcategories and not all start at "01". This was a decision made by NIST during the review process in lieu of renumbering all of the Subcategories. It is not a typographical error in this document.

Function & Category	Category Identifier	Subcategory		SCS 9001 Requirement/ Control
Govern (GV): The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.				
Organizational Context The circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood.	GV.OC	GV.OC-01	The organizational mission is understood and informs cybersecurity risk management.	5.2.1
		GV.OC-02	Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered.	6.1.8, 8.2.6
		GV.OC-03	Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed.	5.2.2[5]
		GV.OC-04	Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated.	8.2.6, 8.3.4, 6.1.8, 7.4.3, 8.4.7
		GV.OC-05	Outcomes, capabilities, and services that the organization depends on are understood and communicated.	6.1.12, 8.1.3
Risk Management Strategy The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions.	GV.RM	GV.RM01	Risk management objectives are established and agreed to by organizational stakeholders	8.1.2, 8.4.1
		GV.RM02	Risk appetite and risk tolerance statements are established, communicated, and maintained	6.1.8, 6.1.4
		GV.RM-03	Cybersecurity risk management activities and outcomes are included in enterprise risk management processes	8.1.2
		GV.RM-04	Strategic direction that describes appropriate risk response options is established and communicated	5.1.1
		GV.RM-05	Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties	6.1.11, 6.1.1
		GV.RM-06	A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated	6.1.7, 8.1.3
		GV.RM-07	Strategic opportunities (i.e., positive risks) are characterized and are included in organizational cybersecurity risk discussions	5.2.1, 5.2.2, 6.1.12

Function & Category	Category Identifier	Subcategory		SCS 9001 Requirement/ Control
Roles, Responsibilities, and Authorities Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated.	GV.OC	GV.OC-01	Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated.	5.2.1
		GV.OC-02	Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered.	6.1.8, 8.2.6
		GV.OC-03	Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed.	5.2.2[5]
		GV.OC-04	Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated.	8.2.6, 8.3.4, 6.1.8, 7.4.3, 8.4.7
Policy Organizational cybersecurity policy is established, communicated, and enforced.	GV.PO	GV.PO-01	Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced.	5.2.1, 5.2.2
		GV.PO-02	Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission.	6.1.1[6]
Oversight Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy.	GV.OV	GV.OV-01	Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction.	6.1.1, 8.1.2
		GV.OV-02	The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks.	6.1.1, 8.1.2
		GV.OV-03	Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed.	6.1.1, 8.1.2
Cybersecurity Supply Chain Risk Management Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders.	GV.SC	GV.SC-01	A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders.	6.1.6, 6.1.7, 6.1.9, 8.1.2
		GV.SC-02	Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally.	5.2.4, 5.3
		GV.SC-03	Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes.	6.1.6, 6.1.7, 6.1.9
		GV.SC-04	Suppliers are known and prioritized by criticality.	6.1.1, 6.1.12, 8.4.1
		GV.SC-05	Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties	4.4.1, 4.4.2, 8.4.1
		GV.SC-06	Planning and due diligence are performed to reduce risks before entering into	8.2.6, 8.4.4
		GV.SC-07	formal supplier or other third-party relationships	4.1.1, 4.2.1, 8.4.4, 8.4.5
		GV.SC-08	The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship	8.4.4, 8.5.5
		GV.SC-09	Relevant suppliers and other third parties are included in incident planning,	4.1.1, 8.3.4, 8.5, 9.1.2, 9.2
		GV.SC-10	response, and recovery activities	8.4.4

Function & Category	Category Identifier	Subcategory		SCS 9001 Requirement/ Control
IDENTIFY (ID): The organization's current cybersecurity risks are understood				
Asset Management (ID. AM): Assets (e.g., data, hardware, software, systems, facilities, services, people) 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	ID.AM	ID.AM-01	Inventories of hardware managed by the organization are maintained.	6.1.2
		ID.AM-02	Inventories of software, services, and systems managed by the organization are maintained.	6.1.2
		ID.AM-03	Representations of the organization's authorized network communication and internal and external network data flows are maintained.	8.1.4
		ID.AM-04	Inventories of services provided by suppliers are maintained.	8.4.4
		ID.AM-05	Assets are prioritized based on classification, criticality, resources, and impact on the mission.	6.1.2
		ID.AM-07	Inventories of data and corresponding metadata for designated data types are maintained.	6.1.2
		ID.AM-08	Systems, hardware, software, services, and data are managed throughout their life cycles.	8.1.1
Risk Assessment (ID. RA): The cybersecurity risk to the organization, assets, and individuals is understood by the organization	ID.RA	ID.RA-01	Vulnerabilities in assets are identified, validated, and recorded	8.1.3
		ID.RA-02	Cyber threat intelligence is received from information sharing forums and sources	6.1.6, 8.3.5
		ID.RA-03	Internal and external threats to the organization are identified and recorded	6.1.6, 8.3.5
		ID.RA-04	Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded	8.1.3, 8.3.16
		ID.RA-05	Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization	8.1.3
		ID.RA-06	Risk responses are chosen, prioritized, planned, tracked, and communicated	6.1.8
		ID.RA-07	Changes and exceptions are managed, assessed for risk impact, recorded, and tracked	8.1.2
		ID.RA-08	Processes for receiving, analyzing, and responding to vulnerability disclosures are established	8.1.3
		ID.RA-09	The authenticity and integrity of hardware and software are assessed prior to acquisition and use	8.3.10, 8.3.12
		ID.RA-10	Critical suppliers are assessed prior to acquisition	8.4.1, 8.4.4, 9.1.2, 9.3.2
Improvement (ID. IM): Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all CSF Functions	PR.AA	ID.IM-01	Improvements are identified from evaluations	9.1.1, 9.1.2
		ID.IM-02	Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties	8.3.6, 8.3.9, 8.4.6
		ID.IM-03	Improvements are identified from execution of operational processes, procedures, and activities	9.1.2, 9.3.2, 9.3.3, 10.1
		ID.IM-04	Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved	8.5.5, 8.5.6

Function & Category	Category Identifier	Subcategory		SCS 9001 Requirement/ Control
PROTECT (PR): Safeguards to manage the organization's cybersecurity risks are used				
Identity Management, Authentication, and Access Control (PR.AA): Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access	PR.AA	PR.AA-01	Identities and credentials for authorized users, services, and hardware are managed by the organization	5.2.7
		PR.AA-02	Identities are proofed and bound to credentials based on the context of interactions	5.2.7, 6.1.13
		PR.AA-03	Users, services, and hardware are authenticated	6.1.13
		PR.AA-04	Identity assertions are protected, conveyed, and verified	5.2.7, 6.1.13, 8.4.7
		PR.AA-05	Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	5.2.8, 5.3.3, 6.1.13
		PR.AA-06	Physical access to assets is managed, monitored, and enforced commensurate with risk	6.1.1, 8.1.4, 8.1.5, PE-1, PE-2, PE-10, PE-11
Awareness and Training (PR.AT): The organization's personnel are provided with cybersecurity awareness and training so that they can perform their cybersecurity-related tasks	PR.AT	PR.AT-01	Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind	7.3.1
		PR.AT-02	Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind	7.3.1
Data Security (PR.DS): Data are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information	PR.DS	PR.DS-01	The confidentiality, integrity, and availability of data-at-rest are protected	5.2.12
		PR.DS-02	The confidentiality, integrity, and availability of data-in-transit are protected	5.2.12
		PR.DS-10	The confidentiality, integrity, and availability of data-in-use are protected	5.2.12
		PR.DS-11	Backups of data are created, protected, maintained, and tested	6.1.11, 8.1.8
Platform Security (PR.PS): The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability	PR.PS	PR.PS-01	Configuration management practices are established and applied	8.3.3, 8.3.16
		PR.PS-02	Software is maintained, replaced, and removed commensurate with risk	5.2.10, 6.1.2, 8.5.3, MA-1
		PR.PS-03	Hardware is maintained, replaced, and removed commensurate with risk	8.1.1, 8.5.11, MA-1
		PR.PS-04	Log records are generated and made available for continuous monitoring	7.6.6, 8.1.5, AU-2, AU-6
		PR.PS-05	Installation and execution of unauthorized software are prevented	5.2.10, 8.5.3
		PR.PS-06	Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle	8.1.5, 8.3.2
Technology Infrastructure Resilience (PR.IR): Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability, and organizational resilience	PR.IR	PR.IR-01	Networks and environments are protected from unauthorized logical access and usage	5.2.7, 5.2.8, 6.1.13, 8.1.4
		PR.IR-02	The organization's technology assets are protected from environmental threats	6.1.1, 6.1.11, 6.1.12, DC-4, PE-6
		PR.IR-03	Mechanisms are implemented to achieve resilience requirements in normal and adverse situations	6.1.11, 8.1.4, 8.1.5, PE-6
		PR.IR-04	Adequate resource capacity to ensure availability is maintained	8.1.4

Function & Category	Category Identifier	Subcategory		SCS 9001 Requirement/ Control
DETECT (DE): Possible cybersecurity attacks and compromises are found and analyzed				
Continuous Monitoring (DE.CM): Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events	DE.CM	DE.CM-01	Networks and network services are monitored to find potentially adverse events	8.1.4, 8.5.3, 8.5.4, 8.5.8
		DE.CM-02	The physical environment is monitored to find potentially adverse events	8.1.4, DC-4
		DE.CM-03	Personnel activity and technology usage are monitored to find potentially adverse events	8.5.3, 8.5.8, SI-1, SP-3
		DE.CM-06	External service provider activities and services are monitored to find potentially adverse events	8.4.4, 8.5.3, 8.5.8
		DE.CM-09	Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events	8.1.4, 8.1.5, 8.5.3, 8.5.4, SI-6
Adverse Event Analysis (DE.AE): Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents		DE.AE-02	Potentially adverse events are analyzed to better understand associated activities	8.3.9, 8.5.5
		DE.AE-03	Information is correlated from multiple sources	6.1.6, 6.1.7, 6.1.12, AU-4
		DE.AE-04	The estimated impact and scope of adverse events are understood	6.1.12
		DE.AE-06	Information on adverse events is provided to authorized staff and tools	5.1.1, 5.2.1, 6.2.1
		DE.AE-07	Cyber threat intelligence and other contextual information are integrated into the analysis	6.1.6, 6.1.7, 6.1.12
		DE.AE-08	Incidents are declared when adverse events meet the defined incident criteria	8.5.5, 8.5.6
RESPOND (RS): Actions regarding a detected cybersecurity incident are taken				
Incident Management (RS.MA): Responses to detected cybersecurity incidents are managed	RS.MA	RS.MA-01	The incident response plan is executed in coordination with relevant third parties once an incident is declared	8.5.5, 8.5.6
		RS.MA-02	Incident reports are triaged and validated	8.5.5, 8.5.6
		RS.MA-03	Incidents are categorized and prioritized	8.5.5, 8.5.6
		RS.MA-04	Incidents are escalated or elevated as needed	8.5.5, 8.5.6
		RS.MA-05	The criteria for initiating incident recovery are applied	8.5.5, 8.5.6
Incident Analysis (RS.AN): Investigations are conducted to ensure effective response and support forensics and recovery activities	RS.AN	RS-AN-03	Analysis is performed to establish what has taken place during an incident and the root cause of the incident	8.5.5, 8.5.6, 10.2.1
		RS-AN-06	Actions performed during an investigation are recorded, and the records' integrity and provenance are preserved	8.5.5, 8.5.6
		RS-AN-07	Incident data and metadata are collected, and their integrity and provenance are preserved	8.5.5, 8.5.6
		RS-AN-08	An incident's magnitude is estimated and validated	8.5.5, 8.5.6
Incident Response Reporting and Communication (RS.CO): Response activities are coordinated with internal and external stakeholders as required by laws, regulations, or policies	RC.CO	RC.CO-02	Internal and external stakeholders are notified of incidents	6.1.11, 8.2.4, 8.2.5
		RC.CO-03	Information is shared with designated internal and external stakeholders	7.4.1, 8.4.4, 8.5.5
Incident Mitigation (RS.MI): Activities are performed to prevent expansion of an event and mitigate its effects	RS.MI	RS.MI-01	Incidents are contained	8.5.5, 10.2.1
			Incidents are eradicated	10.2.1

Function & Category	Category Identifier	Subcategory		SCS 9001 Requirement/ Control
RECOVER (RC): Assets and operations affected by a cybersecurity incident are restored				
Incident Recovery Plan Execution (RC.RP): Restoration activities are performed to ensure operational availability of systems and services affected by cybersecurity incidents	RC.RP	RC.RP-01	The recovery portion of the incident response plan is executed once initiated from the incident response process	8.5.5, 10.2.1
		RC.RP-02	Recovery actions are selected, scoped, prioritized, and performed	8.5.5, 10.2.1
		RC.RP-03	The integrity of backups and other restoration assets is verified before using them for restoration	6.1.11, 8.1.8,
		RC.RP-04	Critical mission functions and cybersecurity risk management are considered to establish post-incident operational norms	6.1.11, 8.5.5
		RC.RP-05	The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed	6.1.11, 8.5.5
		RC.RP-06	The end of incident recovery is declared based on criteria, and incident related documentation is completed	6.1.11, 8.5.5
Incident Recovery Communication (RC.CO): Restoration activities are coordinated with internal and external parties	RC.CO	RC.CO-03	Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders	6.1.11, 8.5.5
		RC.CO-04	Public updates on incident recovery are shared using approved methods and messaging	7.4.1, 8.5.5[7]

Table 2 – CSF 2.0 To SCS 9001 Mapping

SCS 9001 SUPPLY CHAIN SECURITY REQUIREMENTS EXTENDING BEYOND CSF SUBCATEGORIES

SCS 9001 is a complete cyber and supply chain security management system for the ICT industry. The intended applications of SCS 9001 extend beyond that of the CSF.

A partial list of SCS 9001 capabilities beyond the CSF follow:[8]

- **Corporate Principles of Trust:** assessing supplier integrity through querying of specific business practices as part of the organization's public profile
- **Zero Trust Network Architecture (ZTA):** the requirement to have a plan to deploy a ZTA to protect network access and communications.
- **Asset Inventory DB and Management:** establishing a comprehensive database of all organizational a to ensure management, maintenance and fast response upon a security incident.
- **Top management governance:** defining the expectations of organizational management in the definition, support of, review of and communication of the organization's supply chain security goals.
- **Media Management Policy:** effective approaches to managing media and information including disposition of assets.
- **Workspace Policy:** requirements on securing the workspace of employees.
- **Mobile Device and Bring Your Own Device (BYOD) Policies:** requirements for the secure use of mobile, remote and employee-owned devices accessing organizational assets.

- **Cryptographic Control Policies:** policies for the effective use of Cryptography in protecting organizational assets.
- **Counterfeit Parts Mitigation Policy:** requirements for managing parts and specifically unauthorized and potentially fraudulent parts.
- **Business Impact Analysis (BIA):** conducting a BIA to determine risks impacting the organization's ability to operate.
- **Business Continuity Planning (BCP):** establishing a BCP strategy aligned with the BIA on how to resume operations after a security incident or other adverse situations.
- **Secure Network and Systems Planning:** requirements to ensure the secure operation of the organization's networks and systems.
- **Secure Wireless Network Procedures:** requirements to ensure the secure operation of the organization's wireless networks.
- **Access Control & Least Privilege Policies:** requirements to limit access to critical assets.
- **Software Provenance:** requirements to ensure that software components are traceability to their origin to ensure authenticity.
- **Software Bill of Materials (sBOM):** requirements to provide an sBOM in support of products delivered to customers.
- **Hardware Provenance:** requirements to ensure that hardware components are traceability to their origin to ensure authenticity.
- **Hardware Bill or Materials (hBOM):** requirements to provide an hBOM in support of products delivered to customers.
- **Supply Chain Security Processes:** extensive support for supply chain security including requirements such as extending requirements to suppliers, informing customers of security design changes, component substitution, verification of externally provided parts, products and services, supplier selection, expectations of data sub-processors, risk identification, analysis, and treatment, logistics, transportation and storage of materials, as examples.
- **Secure Development Lifecycle:** requirements for the development process to ensure security is considered and security requirements traceable during all phases from conception through product release and deployment and ultimately retirement and disposition of assets.
- **Security Awareness Training:** human resource training and competency assessment including employees and contractors to supply chain security requirements (as opposed to cybersecurity training).
- **Technical Vulnerability Management:** Processes, documented procedures, and measures to detect technical vulnerabilities within organizationally owned or managed assets with use of a risk-based model for prioritizing remediation of identified security vulnerabilities.

CONCLUDING REMARKS

The U.S. government is demanding improvements in cybersecurity and supply chain risk management from the ICT industry. In some cases, industry is incentivized to improve its security posture through programs such as the U.S. BEAD program, and in other cases through the potential of more direct intercession using regulations and new legislation.

The NIST Cybersecurity Framework is a globally embraced publication that is effective in helping organizations manage cybersecurity risk. As stated within the CSF itself, its purpose is to provide **guidance** on how to manage cybersecurity risks. It DOES NOT prescribe how outcomes should be achieved. The current version of the CSF has added 10 Subcategories in support of supply chain security risk management. These Subcategories represent a limited baseline in consideration of supply chain security risk management. By themselves they are insufficient to implement a comprehensive supply chain security management system.

SCS 9001 is a process-based, certifiable global standard. It DOES prescribe how outcomes can be achieved through the implementation of its defined policies, processes, requirements and controls. It was developed to provide assurance that the providers of network products and services can be trusted and operate their businesses with a high level of transparency. It was developed to support network operators of all types to evaluate their suppliers and to provide a higher level of assurance that their vendors:

- Are trustworthy,
- Conduct all aspects of operations and product development with a high level of security,
- Deliver products that are inherently higher in security and quality,
- Deliver consistent and reliable results, and
- Have made requisite investments to support products through their entire lifecycle, including the ability to more quickly identify, mitigate and resolve vulnerabilities found post-deployment.

In turn, all organizations can benefit with an SCS 9001 certification to:

- Improve its security posture to protect itself against cyber and supply chain attacks,
- Protect its brand and future business outcomes,
- Avoid potential litigation and class-action lawsuits,
- Demonstrate its security commitment to their own customers,
- Gain a competitive advantage by building a reputation as a trustworthy vendor, and
- Demonstrate its alignment to, and support of, other non-certifiable publications and frameworks such as the CSF which are not certifiable.

While it is the position of TIA that an independent (3rd party) certification provides the highest level of assurance in evaluating suppliers, we do not mandate that SCS 9001 is only used in independent certifications. Organizations will find value in leveraging the standard to assess their own internal processes and in other conformity assessment models.

Finally, for organizations who have or are considering embracing the CSF, but require a higher level of assurance that their practices follow the recommendations stated therein, Table 2 within this document demonstrates that a certification to SCS 9001 provides a high level of assurance that an organization's security practices align with the recommendations of the CSF while providing substantial additional value in securing their supply chain. A certification to SCS 9001 provides assurance that the certifying organization has achieved the CSF's highest level of implementation, the Tier 4 Adaptive Implementation Tier.

SCS 9001 can be used effectively to demonstrate that an organization's security practices have successfully operationalized the recommendations of the NIST Cybersecurity Framework.

TO LEARN MORE ABOUT TIA SUPPLY CHAIN SECURITY STANDARD, CONTACT US AT: SUPPLYCHAINSECURITY@TIAONLINE.ORG

FOOTNOTES

[1] Note that subsequent to the publishing of the NOFO, NIST has released a significant update of the CSF, Version 2.0. This paper examines this latest version. BEAD Subgrantees must deliver operating plans reflecting the recommendations within the CSF 2.0, now that it has been released.

[2] This Technical Bulletin has a focus on the NIST Cybersecurity Framework. Technical Bulletins contrasting SCS 9001 to the other BEAD NOFO Baseline Requirements are under development. Refer to the TIA QuEST Form SCS 9001 web site for availability: TIA Supply Chain Security Program | TIA Online.

[3] Certain content and graphics in this section are taken directly from NIST publications for ease of reference. The description of the CSF Functions is abbreviated; consult the full CSF 2.0 document (link in the References section) for a full description.

[4] Consult the TIA QuEST Forum web site at TIA Supply Chain Security Program | TIA Online for an Industry Report providing an introduction of many popular contemporary security works and other Technical Bulletins providing a detailed comparison of other standards, publications and frameworks to SCS 9001 amongst other collateral.

[5] Many other requirements have an element of legal, regulatory and contractual requirements. SCS 9001 does not have requirements centered on civil liberties.

[6] SCS 9001 identifies a number of policies for managing various elements of cyber and supply chain security risk.

[7] SCS 9001 infers public updates through the establishment of an incident management process including to whom and what to communicate which may or may not include public notifications. However, it is non-explicit as to making public announcements beyond its requirements of identifying all stakeholders with whom updates should be provided. This is an area for future enhancement including consideration of global government initiatives on requiring public disclosure of security events for critical infrastructure with the U.S. Government's Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) being one example. More information is available at: Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) | CISA.

[8] This is a partial list. SCS 9001 is a large and comprehensive standard. Identifying and describing every requirement in detail is beyond the scope of this Tech Bulletin.

REFERENCES

NIST Cybersecurity Framework (home page) — Cybersecurity Framework | NIST

NIST Cybersecurity Framework V2.0 (full document) — NIST.CSWP.29.pdf

U.S. Government BEAD Program — Broadband Equity, Access, and Deployment (BEAD) Program | BroadbandUSA (doc.gov)

BEAD Program Notice of Funding Opportunity (NOFO) — BEAD NOFO.pdf (doc.gov)

U.S. Executive Order 13636 — Executive Order — Improving Critical Infrastructure Cybersecurity | whitehouse.gov (archives.gov)

U.S. Executive Order 14028 — DCPD-202100401.pdf (govinfo.gov)