TIA QuEST Forum
Telecommunications Industry Association
TECHNICAL BULLETIN
TIAonline.org / @TIAonline

How TIA QuEST Forum's SCS 9001 Supply Chain Security Standard Operationalizes the National Institute of Standards and Technology Publication "*NISTIR 8276 Key Practices In Cyber Supply Chain Risk Management: Observations from Industry*"

July 2022

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. Recent examples include U.S. Executive Order EO14028 and the U.K.'s Telecommunications Security Act of 2021.

As an example of government influence, 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 through-out 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) 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"*.

This TIA Technical Bulletin provides an overview of NIST's NISTIR 8276 publication and how the Telecommunications Industry Associate (TIA) QuEST Forum's SCS 9001 Supply Chain Security Standard can assist in realizing 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 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 built 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.

SCS9001 is the first comprehensive, measurable, and independently certifiable process-based supply chain security standard for the ICT industry and 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.

Overview of NIST NISTIR 8276

This NIST publication is based on NIST research into cyber supply chain risk management, numerous standards, industry best practices and interviews conducted with companies in 2015 and 2019 on their supply chain security practices and experiences.

These interviews led to the development of 24 case studies. NISTIR 8276 provides a summary of practices identified by subject matter experts to serve as the foundation of an effective cyber supply chain risk management program. NISTIR 8276 was updated and released in February 2021.

NISTIR 8276 notes that identifying, assessing, and mitigating cyber supply chain risks is a critical capability in achieving improved business resilience and that the multidisciplinary approach espoused be referred to as Cyber Supply Chain Risk Management (C-SCRM).

NISTIR 8276 promotes a set of Key Practices that organizations of any size, complexity or maturity can leverage to manage cybersecurity risks associated with their supply chains.

The identified Key Practices are:

1. Integrate C-SCRM Across the Organization
2. Establish a Formal C-SCRM Program
3. Know and Manage Critical Suppliers
4. Understand the Organization's Supply Chain
5. Closely Collaborate with Key Suppliers
6. Include Key Suppliers in Resilience and Improvement Activities
7. Assess and Monitor Throughout the Supplier Relationship
8. Plan for the Full Life Cycle

In addition to the Key Practices, NISTIR 8276 also identifies 24 Recommendations. This Bulletin provides an overview of how SCS 9001 is aligned with the Key Practices and Recommendations.

How SCS 9001 Aligns with NISTIR 8276

The following table identifies the Key Practices defined within NISTIR 8276 and demonstrates how SCS 9001 can effectively operationalize them.[1]

NISTIR 8276 Key Practice	TIA QuEST Forum SCS 9001 Alignment
Integrate C-SCRM Across the Organization	
This Key Practice encourages that organizations establish Supply Chain oversight across the entire organization including executive support from supply chain/procurement, information technology, cybersecurity, operations, legal, enterprise risk management (ERM), and other functional and leadership areas.	SCS 9001 is a Supply Chain Security standard which assures that organizations operate with transparency, integrity and have proper operational controls in place to provide a higher level of confidence in their ability to supply products and services of inherently higher security.
Risks should be reviewed, and risk mitigation plans established, priorities set, and sharing of best practices should be shared across the organization.	SCS 9001 additionally provides coverage for addressing the complete supply chain of vendors including all of their suppliers.
Establish a Formal C-SCRM Program	
This Key Practice recommends establishment of a formal C-SCRM program to ensure accountability for managing cyber supply chain risks. Twenty-four high-level characteristics of a formal C-SCRM program are provided for organizations to consider adopting. These characteristics follow along with examples on how SCS 9001 is aligned with the identified characteristics.	SCS 9001 is a certifiable standard and can be the basis for providing assurance that organizations have established an effective C-SCRM program.
- Increased Executive Board or Executive Level involvement for establishing C-SCRM as a top business priority and to ensure proper oversight	SCS 9001 requires that Top Management be responsible for the organization’s Supply Chain Security implementation including setting the strategy, assessing the effectiveness of the strategy as part of a regular management review, ensuring that all responsibilities are defined and that policies are communicated and understood at all levels of the organization
- Clear governance of C-SCRM activities that includes cross-organizational roles and responsibilities with clear definitions and designation/distribution of these roles among enterprise risk management, supply chain, cybersecurity, product management and product security (if applicable), and other relevant functions appropriate for the organization’s business	SCS 9001 requires that Top Management communicate all policies and responsibilities of the organization’s C-SCRM program through all impacted levels of the organization.

[1] Excerpts from NISTIR 8276 are used in the table identifying Key Practices

- Standards-based policies and procedures that provide guidance to different business units detailing their C-SCRM activities	SCS 9001 defines policies and procedures as requirements that must be fully documented and regularly reviewed for effectiveness with continuous improvement required, and that all such policies and procedures are fully communicated to impacted business units.
- Same policies used internally and with suppliers	SCS 9001 requires that organizations establish methods to ensure external suppliers meet security requirements. These requirements are at the discretion of the organization to meet their business needs but include needs such as measures to enable effective governance, legal, statutory and regulatory compliance, policies to ensure requirements are extended to the full extent of the supply chain, regular monitoring, review and / or audit of supplier service delivery.
- Integration of cybersecurity considerations into the system and product development life cycle	SCS 9001 requires that suppliers implement a secure product delivery process and that these requirements are extended to outsourced development.
- Use of cross-functional teams to address specific enterprise-wide risks	SCS 9001 requires that supply chain security requirements be implemented across all organizational functions responsible for implementing the C-SCRM program.
- Clear definition of roles of individuals responsible for cybersecurity aspects of supplier relationships (which may be different than those responsible for procurement activities with specific suppliers)	SCS 9001 requires that organizational roles, responsibilities, and authorities be clearly assigned, communicated and understood throughout the organization.
- Establishment of centers of excellence to identify and manage best practices	SCS 9001 does not explicitly require the establishment of centers of excellence. This is inferred by other requirements throughout the standard. Additionally, the standard requires that all participating individuals be trained and deemed competent in the execution of their duties.
- A set of measures of success used to facilitate decision-making, accountability, and improvement	SCS 9001 defines dozens of controls and promotes benchmarking whereby certified organizations collect and report a variety of key operational metrics to demonstrate continuous improvement.
- Approved and banned supplier lists	SCS 9001 provides requirements in the selection of external suppliers including the regular assessment of suppliers, a process for assessing supplier risk, and a process for obtaining approvals prior to supplier selection.
- Use of software and hardware component inventory (e.g., bill of materials) for third-party components	SCS 9001 requires that organizations receive BOMs from suppliers along with other provenance and traceability records.

- Prioritization of suppliers based on their criticality	SCS 9001 promotes selection of suppliers based on responses to Corporate Principles of Trust (the integrity in which they conduct business operations) as well as Extent of Control of External Providers through which suppliers are vetted as to meeting the security requirements of the organization.
- Establishment of testing procedures for the most critical components	SCS 9001 requires that organizations establish processes to perform testing to ensure that purchased products meet specifications and also to ensure that product changes or substitutions do not adversely affect conformity to requirements, security, or performance.
- Establishment of a known set of security requirements or controls for all suppliers, especially robust security requirements for critical suppliers to be used in procurement (sometimes known as master specifications)	SCS 9001 requires documented procedures to ensure that suppliers comply with contractual, legal, statutory, protection of intellectual property and regulatory requirements. The standard also sets a variety of other expectations such as suppliers proper vetting of employees, supplier employee training, defining security requirements through the lifetime of the business relationship, protection of sensitive data, and traceability of components, amongst other topics.
- Service-level agreements (SLA) with suppliers that state the requirements for adhering to the organization's cybersecurity policy and any controls required of the supplier	SCS 9001 requires that organizations establish methods to ensure suppliers meet security requirements. These methods are comprehensive and cover a variety of needs such as: agreement to security, service, and capacity-level requirements, primary points of contact, measures to implement to enable effective governance, risk management, legal and regulatory compliance, reassessment of risk for supplier changes in methods, products, or services, notification of security incidents, and controls, processes, or policies that ensure requirements are extended to all levels of the supply chain.
- Establishment of intellectual property rights agreements	SCS 9001 requires that organizations establish requirements with suppliers including Legal, Statutory, Regulatory, and Contractual Requirements
- Shared supplier questionnaires across like organizations, such as within the same critical infrastructure sector	SCS 9001 requires that organizations vet their suppliers. The standard does not explicitly call out the development of a shared questionnaire; it leaves the process of vetting suppliers up to the organization provided that the requirements of the standard are met.

- Upstream propagation of acquirer's security requirements within the supply chain to subtier suppliers	SCS 9001 requires that all conditions expected of each upstream supplier be extended fully through the supply chain to ensure traceability to the origin of all components.
- Assurance that suppliers have only the access they need in terms of data, capability, functionality, and infrastructure; bounding this access by specific time frames during which suppliers need it	SCS 9001 identifies Access Control Policies for ensuring appropriate identity, entitlement, and access management for all corporate assets including access given to external parties such as partners and suppliers. Additionally, access credentials are governed through their lifecycle including removal of access upon termination of the business relationship.
- Use of escrow services for suppliers with a questionable or risky track record	SCS 9001 requires that organization define and execute Supply Chain Security Risk Assessment, Security Risk Analysis, and Supply Chain Security Mitigation processes. While the standard does not explicitly call out the use of escrow services for questionable suppliers, this approach can be inferred as one possible action to protect the organization's supply chain.
- Provision of organization-wide training for all relevant stakeholders within the organization, such as supply chain, legal, product development, and procurement; this training may also be extended to key suppliers	SCS 9001 requires that organizations sufficiently train their employees including specific attention to security awareness training to ensure competency of all individuals taking part in corporate functions with such a need.
- Identification of alternative sources of critical components to ensure uninterrupted production and delivery of products	SCS 9001 requires that organization define and execute Supply Chain Security Risk Assessment, Security Risk Analysis, and Supply Chain Security Mitigation processes. While the standard does not explicitly call out identification of alternative sources of critical components, this approach can be inferred as one possible action to protect the organization's supply chain. In general, the use of single sourced components is discouraged when it can be avoided.
- Secure requirements guiding disposal of hardware that contains regulated data such as personally identifiable information [PII] or protected health information [PHI]) or otherwise sensitive information (e.g., intellectual property)	SCS 9001 has an extensive set of requirements as part of the required Media Management Policy including the proper sanitization of storage devices as part of their disposal.
- Protocols for securely terminating supplier relationships to ensure that all hardware containing acquirer's data has been properly disposed of and that the risks of data leakage have been minimized	SCS 9001 requires that the organization formalize their supplier relationships and define expectations through the entirety of the relationship including requirements to address the expiration of the relationship and proper treatment of the organization's sensitive data.

Know and Manage Critical Suppliers	
This Key Practice defines critical suppliers as those which, if disrupted, would 'create a negative business impact on the organization'.	SCS 9001 requires that the organization review and document their Supply Chain Security Risk Assessment, Security Risk Analysis and Supply Chain Security Risk Mitigation processes.
Criteria are provided to help determine if a supplier is critical such as consideration of the supplier's financial stability, access to regulated data of the organization, and access to the organization's systems and network infrastructure, as examples.	SCS 9001 requires that certifying organizations respond to questions on the integrity and transparency of their business operations through an assessment of Corporate Principles of Trust whereby the supplier addresses questions on the independence of their BOD, whether financial results are independently audited, disclosure of prior legal judgements against the company and whether the company is unduly influence by any government or government agencies, amongst other topics.
Understand the Organization's Supply Chain	SCS 9001 defines and requires numerous operational processes to assess and improve supply chain security. Organizations are expected to engage with their suppliers in meeting required supply chain security requirements.
This Key Practice states, in consideration of the global nature of today's complex supply chains, that organizations must have a deep understanding of their supply chains in however many layers deep as is necessary.	Organizations are required to have a Control Plan and source products and components that are new and authentic and purchased from the original manufacturer or authorized external providers. Organizations leveraging provenance policies and traceability, are expected to be able to track all products / components to the original source to prevent the use of counterfeit and suspect parts. The Control Plan shall specify the extension of applicable requirements to the organization's suppliers, contractors, and their subcontractors.
Organizations exhibiting best practices must have visibility into the operations of their suppliers in order to assess their operations in order to:	
Capture quality data	SCS 9001 requires that the organizations establish verification processes to determine and perform testing to ensure purchased material/parts meet specified requirements, not limited to quality data but additionally that purchased products meet security and regulatory requirements as additional examples. Other artifacts are also defined and can be demanded from suppliers such as Software Bills of Materials and full test results across a variety of test methodologies.
Leverage tools to assess inventory and validate provenance claims anywhere within the supply chain.	SCS 9001 requires methods to ensure software identification and traceability for all software, firmware, and supporting logic. Special emphasis is made on products using open-source components. A variety of techniques are suggested. Further, SCS 9001 requires traceability of components of all types through its

	complete supply chain in order to guard against corrupted components and counterfeits with numerous requirements identified to cover all types of components.
Have insight into how suppliers vet their personnel	SCS 9001 requires that organizations assess their suppliers in how they evaluate their employees through a Security Awareness Training Human Resource (HR) Security Policy that include documented roles and responsibilities of contractors, employees, and third-party users as they relate to supply chain assets and security, methods for screening/background verification checks on all candidates for employment in accordance with relevant laws, regulations, and ethics proportional to the business, methods for screening/background verification for individuals prior to authorizing access to organizational systems, and contractual agreements with personnel stating their responsibilities including for security.
Closely Collaborate with Key Suppliers	
This Key Practice encourages organizations to establish close relationships with suppliers including the creation of complete ecosystems to improve the coordination of and simplification of complex supply chains.	SCS 9001 recognizes the need for collaboration between not only all functions within an organization responsible for the C-SCRM program, but additionally between the organization, their suppliers, and their suppliers in achieving the goals of the C-SCRM program.
Include Key Suppliers in Resilience and Improvement Activities	
This Key Practice concludes that threat actors target organizations through their supply chains, but threats to those supply chains can also include environmental risks and geopolitical unrest. Further, mature organizations have formal continuous improvements processes that include their critical suppliers.	SCS 9001 requires that organizations extend their security and supply chain requirements to their suppliers, and that they work collaboratively with those suppliers in the establishment, review and continuous improvement of all elements of the supplier relationship.
Assess and Monitor Throughout the Supplier Relationship	
This Key Practice establishes that organizations, their environments, and supply chains are continuously evolving.	SCS 9001 requires numerous organizational processes be established such as Security Planning, Supply Chain Security Risk Assessment, Technical Vulnerability, Business Impact Analysis and Business Continuity Planning. Organizations certified to SCS 9001 will be assessed on all of these requirements which are expected to be reviewed for effectiveness and improved at least annually.

Accordingly, supplier assessments and periodic re-assessments should be performed over the complete duration of the relationship. A variety of assessment approaches are identified, including self-assessment, supplier attestation, third-party assessments, formal certifications, and site visits.	TIA is a proponent of independently certifiable standards for topics as important as Supply Chain Security. Upon initial certification, organizations are required to undergo annual surveillance audits in addition to 3-year re-certifications.
Plan for the Full Life Cycle	
This Key Practice identifies the need for business continuity processes to safeguard the organizations operations and to address unexpected interruptions to their supply chains. Examples of such disruptions may include suppliers determining components to be obsolete and no longer manufacturing such components or the supplier adopting a different business direction due to acquisition or change of management.	SCS 9001 requires that organizations implement Business Impact Analysis which includes the loss of consideration of key loss scenarios which may include loss or unavailability of facility, technology, personnel, and suppliers as well as Business Continuity Planning which includes the identification of impacted customers and other business relationships that represent critical intra-supply chain business process dependencies.

How SCS 9001 Aligns with NISTIR 8276 Recommendations

Section 4 of NISTIR 8276 provides 24 recommendations based on conducted case studies as well as other standards and best practice documents.

The following table explains how SCS 9001 operationalizes the Key Practices defined within NISTIR 8276.[2]

NISTIR 8276 Recommendation	TIA QuEST Forum SCS 9001 Alignment
Establish supply chain risk councils that include executives from across the organization (e.g., cyber, product security, procurement, legal, privacy, enterprise risk management, business units, etc.).	SCS 9001 does not explicitly call out an organizational structure such as a 'supply chain risk council', but essentially all requirements within SCS 9001 call out the need for full organizational support across all functions participating in the C-SCRM program, and that Top Management has the responsibility for communicating the program, roles, responsibilities and expectations.
Create explicit collaborative roles, structures, and processes for supply chain, cybersecurity, product security, and physical security functions.	SCS 9001 requires through Security Policies the establishment of a plan and security program inclusive of defined security roles and responsibilities for business leadership and through Human Resource Security Policies that the organization define documented roles and responsibilities of contractors, employees, and third-party users as they relate to supply chain assets and security.
Increase Executive Board involvement in C-SCRM through regular risk discussions and sharing of measures of performance.	SCS 9001 requires that Top Management have responsibility for Supply Chain Security. "Top Management" is intended to indicate the highest level of governance available in the organization regardless of specific organizational corporate structure. Top Management is responsible for setting the organization's supply chain security plan, regular assessment of the effectiveness of the plan, and ensuring that supply chain security responsibilities are communicated to all levels of the organization.
Integrate cybersecurity considerations into the system and product life cycle.	SCS 9001 has requirements to address the cybersecurity of all aspects of a business' operations including IT, product development, and supply chain.
Clearly define roles and responsibilities for the security aspects of specific supplier relationships.	SCS 9001 requires that the organization establish methods to ensure external suppliers meet security requirements including the roles and responsibilities of the supplier.

[2] Excerpts from NISTIR 8276 are used in the table identifying Recommendations

NISTIR 8276 Recommendation	TIA QuEST Forum SCS 9001 Alignment
Use master requirements lists and SLAs to establish requirements with suppliers.	SCS 9001 requires that organizations incorporate into supply chain agreements (e.g., service level agreements) provisions including scope of business relationship and services offered, data exchange and usage, personnel and infrastructure network and systems components for service delivery and support, physical geographical location of hosted services, and known regulatory compliance considerations as appropriate. Performance reviews are expected.
Propagate security requirements to suppliers' sub-suppliers.	SCS 9001 requires that the organization establish methods to ensure external suppliers extend controls, processes, and policies that ensure requirements are extended to their external suppliers as appropriate to mitigate and contain security risks.
Train key stakeholders in the organization and within the supplier's organization.	SCS 9001 requires that employees and contractors responsible for the organization's C-SCRM policy receive appropriate security and security awareness training to ensure they are competent in their function.
Terminate supplier relationships with security in mind.	SCS 9001 requires extensive controls be in place for External Suppliers including requirements to address expiration of the business relationship and treatment of the organization's data and assets.
Use the Criticality Analysis Process Model or BIA to determine supplier criticality.	SCS 9001 requires that organizations conduct a Business Impact Analysis (BIA) to identify all dependencies, including critical applications, business partners, suppliers, and third-party service providers. Key loss scenarios may include but are not limited to loss or unavailability of facility, technology, personnel, and suppliers.
Establish visibility into the suppliers' production processes (e.g., capture defect rates, causes of failure, and testing).	SCS 9001 requires that organizations establish verification processes to determine and perform testing to ensure purchased material/parts meet specified requirements. SCS 9001 also requires production compliance and traceability information be available on demand from suppliers.

NISTIR 8276 Recommendation	TIA QuEST Forum SCS 9001 Alignment
Know if the data and infrastructure are accessible to suppliers' sub-suppliers.	SCS 9001 Least Privilege policies for employing the principle of least privilege to specific business processes which denies network communications traffic by default and only allows by exception and that this be documented and evaluated at least annually for effectiveness. Further, SCS 9001 requires Access Control policies for ensuring appropriate identity, entitlement, and access management for all corporate assets and that users be established, documented, and evaluated at least annually for effectiveness. SCS 9001 requires that all access to data assets and network resources be monitored and logged. Finally, SCS 9001 defines comprehensive Asset Management policies for ensuring that all assets are effectively handled according to the classification scheme adopted by the organization to ensure their security shall be established, documented, and evaluated at least annually for effectiveness. Data assets are encrypted while at rest (storage), in use (memory) and in transit (network transmission).
Mentor and coach suppliers to improve their cybersecurity practices.	SCS 9001 does not call out mentoring of suppliers, but the standard does require close coordination between organizations and their suppliers, that they collaborate on numerous cyber and supply chain risk and technical vulnerability management, that suppliers' employees be trained and proven competent in their function, and that regular review and continuous improvement be achieved.
Require the use of the same standards within both acquirer and supplier organizations.	SCS 9001 is a supply chain security standard that can be applied to both acquirer and supplier organizations to ensure consistency in approaches to C-SCRM.
Use acquirer assessment questionnaires to influence acquirer's cybersecurity requirements.	SCS 9001 does not explicitly call out the use of questionnaires, but their development can be inferred by the substantial processes and requirements called out within the standard.
Include key suppliers in incident response, business continuity, and disaster recovery plans and tests.	SCS 9001 has requirements that all suppliers collaborate in these processes, and many others.
Maintain a watchlist of suppliers who have had issues in the past and about which the acquirer should be cautious for future use (e.g., "Issue Suppliers"). Such suppliers should only be used after approval from the supply chain risk council.	SCS 9001 embraces the notion of Corporate Principles of Trust, through which suppliers are evaluated as to the transparency and integrity in which they operate their businesses.

NISTIR 8276 Recommendation	TIA QuEST Forum SCS 9001 Alignment
Establish remediation acceptance criteria for the identified risks.	SCS 9001 requires that organizations conduct a Supply Chain Security Risk Mitigation process to identify risks, then develop and implement risk mitigation plans. Recognizing that risks can never be fully eliminated, SCS 9001 also promotes that organizations define and publish their Acceptable Level of Risk based on a variety of criteria.
Establish cybersecurity requirements through a Security Exhibit, Security Schedule, or Security Addendum document. This document should be finalized in partnership with the risk council members and included in all master services agreements (MSAs) of all suppliers based on the risk associated with the supplier engagement.	SCS 9001 requires the establishment of numerous operational, physical security, cybersecurity and supply chain security processes, amongst others. SCS 9001 does not call out a specific document to be developed and attached to MSAs, but this need can be inferred from the numerous other processes and produced documentation. SCS 9001 does define numerous controls for managing supplier relationships including an agreement to all relevant security, service, and capacity-level requirements and supply chain agreements (service level agreements) that identify all mutually agreed-upon provisions including, as examples, the scope of the business relationship, roles and responsibilities, sharing of data, asset and network access, and regulatory compliance requirements.
Establish protocols for vulnerability disclosure and incident notification.	SCS 9001 requires that policies, documented procedures and measures be established to detect technical vulnerabilities within organizationally owned or managed applications, infrastructure network and system components and that a risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Additionally, SCS 9001 defines that an Incident Management Process be established to detect and handle security incidents including that customers and other interested parties receive notification and updates for the duration of the incident.
Establish protocols for communications with external stakeholders during incidents.	SCS 9001 requires that organizations establish Incident Management and Incident Reporting Processes whereby all detected incidents be reported to the appropriate personnel and archived. Further, methods are to be developed for the reporting of incidents to customers and users.
Collaborate on lessons learned, and update joint plans based on lessons learned.	SCS 9001 defines numerous processes which are intended to be reviewed regularly, most at least annually, and that all functions contributing to a C-SCRM function work to continuously improve. This expectation extends to suppliers.

NISTIR 8276 Recommendation	TIA QuEST Forum SCS 9001 Alignment
Use third-party assessments, site visits, and formal certification to assess critical suppliers.	SCS 9001 is a certifiable standard which requires organizations seeking certification to engage with an independent 3rd party known as a *Certification Body*). Certification Bodies are responsible for verifying that the organization has implemented an SCS 9001 compliant security management system by visiting site(s) identified within the organization's Statement of Applicability or SoA. The SoA identifies what sites, business processes, functions, and/or products are to be assessed for certification.
Have plans in place for supplied product obsolescence.	SCS 9001 requires that organizations establish a parts obsolescence monitoring program.

Conclusion

SCS 9001 is a Supply Chain Security standard used to certify the proper operational practices of suppliers in delivering products and services of inherently higher security to network operators.

SCS 9001 assists network operators in evaluating their vendors and to determine that vendors:

- operate their businesses with integrity and transparency;
- implement supply chain security processes across their organizations and suppliers;
- conduct all aspects of operations and product development with a high level of security;
- deliver products that are inherently higher in security and quality; 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.

The NOFO is non-specific as to how suppliers should achieve the 'attestation' of meeting the baseline requirements stated therein. As a certifiable standard whereby an independent 3rd party determines an organizations compliance with the standard, SCS 9001 is a powerful tool in helping to meet the NOFO attestation requirements.

Questions? Want more information about TIA QuEST Forum's SCS 9001?
Visit: https://bit.ly/SCS9001
Send us an email: supplychainsecurity@tiaonline.org

References

- NIST NISTIR 8276:
  Key Practices in Cyber Supply Chain Risk Management: Observations from Industry (nist.gov)
- 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)

This document is not a Standard or TSB and does not modify any existing standards. This document is solely meant to communicate ideas and general information to industry.