Before the
U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Gaithersburg, MD, 20899

In the Matter of	)	
	)	
Evaluating and Improving NIST Cybersecurity	)	
Resources: The Cybersecurity Framework and	)	Docket No. 220210-0045
Cybersecurity Supply Chain Risk Management	)	

COMMENTS OF THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION

The Telecommunications Industry Association ("TIA") appreciates the opportunity to provide additional input to the National Institute of Standards and Technology ("NIST") in response to the NIST Cybersecurity Framework 2.0 Concept Paper. TIA recognizes the importance of NIST's Cybersecurity Framework ("Framework" or "CSF"), which provides an invaluable tool for Information and Communications Technology ("ICT") industry efforts to build security into their networks and supply chains.

As we mentioned in our comments in response to NIST's Request for Information on *Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management* ("RFI"), security is at the core of what we do at TIA.[1] TIA represents more than four hundred domestic and global manufacturers and vendors of telecommunications equipment and services – Our members compose the trusted manufacturers and vendors of the ICT industry. TIA is also an ANSI-accredited Standards Development Organization, and we have launched the first standard to drill down and add transparency and trust to the ICT supply chain – SCS 9001.

[1] TIA Comments on NIST RFI (April 25, 2022).

As we mentioned in our RFI comments, TIA has labored over the past few years with industry and input from global government stakeholders to standardize supply chain risk mitigation ("SCRM") best practices to ensure that ICT supply chains are built with security in mind. TIA believes SCS 9001, a process-based standard based on our quality management system capabilities, shows promise to provide a standardized supply chain assurance benchmarked across the ICT marketplace. NIST was correct in their Concept Paper to recognize the value of keeping the CSF's Informative References robust and up to date, so that new standards that are built by the ICT industry between CSF revisions, such as SCS 9001, can still be included as a reference.

TIA is in the process of releasing version 2.0 of SCS 9001, but we agree with the Concept Paper that there is clear value in providing mappings for how Informative Resources relate to the requirements of the CSF. Given SCS 9001 extensive processes focused on zero trust architecture, supplier trust principles, incident management and response all spread across 10 security domains with 54 controls, we can see that there will likely be a significant overlap between the CSF and SCS 9001. As part of our work creating SCS 9001, we have mapped the standard to numerous industry best practices and government resources focused on security – Including version 1.1 of the CSF. In response to the Concept Paper's Call to Action on mapping resources with the CSF, we are pleased to be able to submit our mapping of SCS 9001 to the CSF in the attached Appendix 1.[2] Additionally, we would be very interested in coordinating a mapping of version 2 of SCS 9001, once it is released, with the updated CSF, and look forward to working with NIST on this in the future.

[2] TIA Technical Bulletin: *How TIA QuEST Forum's SCS 9001 Supply Chain Security Standard Operationalizes the National Standards and Technology Cybersecurity Framework 1.1* (available at https://tiaonline.org/what-we-do/technology-programs/supply-chain-security/).

We strongly believe that this standard solves a problem facing both the ICT industry and trusted governments when it comes to identifying risks in the ICT supply chain, and the inclusion of SCS 9001 as an online Informative Reference, in addition to mapping SCS 9001 to the CSF 2.0, can help users understand how to align their SCRM practices within the Framework.

TIA looks forward to continued partnership with NIST as it continues working on this next iteration of the Framework and considers ways to improve its cybersecurity resources and advance cybersecurity supply chain risk management.

By: __*/s/ Colin Andrews*____
Colin Black Andrews
Senior Director, Government Affairs

TELECOMMUNICATIONS INDUSTRY ASSOCIATION
1310 N. Courthouse Road
Suite 800
Arlington, VA 22201
(703) 907-7700

March 3, 2023

Attachments:
Appendix 1: TIA Technical Bulletin Mapping SCS 9001 to NIST's Cybersecurity Framework 1.1

Appendix 1

TIA Technical Bulletin
How TIA QuEST Forum's SCS 9001 Supply Chain Security Standard Operationalizes the National Standards and Technology Cybersecurity Framework 1.1

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 (NIST) Cybersecurity Framework 1.1

August 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, 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 States 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.

Introduction to the National Institute of Standards and Technology and the Framework for Improving Critical Infrastructure Cybersecurity

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.

Recognizing the increasing risk of cyber-attacks, in February 2013, the President issued Executive Order (EO) 13636, "*Improving Critical Infrastructure Cybersecurity*". This EO recognizes that the national and economic security of the United States depends on the reliable operation of critical infrastructure. The critical infrastructure intended for protection was defined in the U.S. Patriot Act of 2015 as:

"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."

The EO directed NIST to work with stakeholders to develop a cybersecurity framework based on existing standards, guidelines, and practices to reduce cyber risks to critical infrastructure. The outcome of this work is the NIST publication "Framework for Improving Critical Infrastructure Cybersecurity" (CSF).

The CSF provides guidance and is based on existing standards, guidelines, and best practices for organizations to improve their operational processes to reduce cybersecurity risk. It is intended to be customized by individual organizations and organizations in response to their specific needs and risks. The CSF has been voluntary for industry prior to the BEAD NOFO but in Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, the CSF was made mandatory for U.S. federal government agencies.

While originally targeted at Critical Infrastructure, the CSF has evolved and can now be widely applied to help protect the network and IT assets of a variety of organizations across many industries.

After EO 13636, the Cybersecurity Enhancement Act of 2014 bill was passed by Congress. This bill reinforces NIST's role as set in EO 13636 and provides for "an ongoing, voluntary public-private partnership to improve cybersecurity, and to strengthen cybersecurity research and

development, workforce development and education, and public awareness and preparedness, and for other purposes."

The current version of the CSF is V1.1 and it was released in April 2018. NIST is currently working on a major update at the time of the writing of this Technical Bulletin, commonly referred to as V2.0.

Overview of the NIST Cyber Security Framework[1]

Organizations can use the CSF to help in identifying, assessing, and managing 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.

The CSF is composed of three components: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles.

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 five Key Functions named 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.

[1] Certain content and graphics in this section are taken from NIST publications.

- 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 it's 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.

NIST released Special Publication 1271, "Getting Started with the NIST Cybersecurity Framework: A Quick Start Guide" in August 2021. SP 1271 is a simplified overview of the CSF publication with a focus on the CSF Core of Key Functions and corresponding Activities.

How SCS 9001 Aligns with the NIST Cybersecurity Framework 1.1

The following table explains how SCS 9001 operationalizes the NIST Cyber Security Framework V1.1.[2] with the comparison being made to the CSF Core as defined in NIST SP 1271.[3] Descriptions in the left columns are taken verbatim from NIST SP 1271 and the color coding used therein is maintained for ease of reference.

CSF 1.1 Key Function	TIA QuEST Forum SCS 9001 Alignment
IDENTIFY Develop an organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. This Key Function identifies 5 activities.	
Identify critical enterprise processes and assets. What are your enterprise's activities that absolutely must continue in order to be viable? For example, this could be maintaining a website to retrieve payments, protecting customer/patient information securely, or ensuring that the information your enterprise collects remains accessible and accurate.	SCS 9001 requires that organizations perform self-assessments and establish policies to identify and mitigate risks such as: • Business Impact Analysis (BIA): determine the key factors on protections of assets and networks. The BIA requires that the organization implement methods for collaboration with external providers on supply chain and security planning activities. • Technical Vulnerability Management: identifying, evaluating, treating, and reporting on security vulnerabilities in systems and software • Risk Assessment and Mitigation: identifying, assessing, and mitigating risks to scope, schedule, cost, security, and quality. Supply Chain Security Risk Assessment: requires that all supply chain assets are included in risk assessment such as information/cyber, network, product/service, development/production, and support assets.

[2] Excerpts from NIST SP 1271 are used in this table. A link to the document is provided in the References section.
[3] The Key Function Activities differ slightly between the CSF V1.1 and NIST SP 1271.

Document information flows It's important to not only understand what type of information your enterprise collects and uses, but also to understand where the data is located and how it is used, especially where contracts and external partners are engaged.	SCS 9001 requires that organizations perform a Security Risk Analysis which includes consideration of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure and limiting access to only those requiring it to perform their job function.
Maintain hardware and software inventory It's important to have an understanding of the computers and software in your enterprise because these are frequently the entry points of malicious actors. This inventory could be as simple as a spreadsheet.	SCS 9001 requires that organizations maintain a comprehensive asset inventory database. Assets shall be recorded as to type and other key criteria such as location, owner, type, release level, patch level, and relationship to other assets, amongst other information. The asset inventory database is a key element of organizational maturity in managing their infrastructure and especially sensitive aspects of that infrastructure that may be subject to cyber-attack. SBOMs are expected to be imported into the database to quickly determine vulnerabilities upon receipt of new cyber risk.
Establish policies for cybersecurity that include roles and responsibilities These policies and procedures should clearly describe your expectations for how cybersecurity activities will protect your information and systems, and how they support critical enterprise processes. Cybersecurity policies should be integrated with other enterprise risk considerations (e.g., financial, reputational).	SCS 9001 requires that organizations implement cyber security policies across the entire enterprise. An Incident Management Process is required that establishes and maintains a documented operational incident response process for organizational systems, products, and services. The process includes a security incident response team(s) with defined roles, responsibilities, competencies, and decision-making authority. On-going communications and updates are required to key stakeholders including customers.
Identify threats, vulnerabilities, and risk to assets Ensure risk management processes are established and managed to ensure internal and external threats are identified, assessed, and documented in risk registers. Ensure risk responses are identified and prioritized, executed, and results monitored.	SCS 9001 defines numerous policies and procedures including technical vulnerability and operational risk management as requirements and that they 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.

PROTECT	
Develop and implement the appropriate safeguards to ensure delivery of services. This Key Function identifies 6 activities.	
Manage access to assets and information Create unique accounts for each employee and ensure that users only have access to information, computers, and applications that are needed for their jobs. Authenticate users (e.g., passwords, multi-factor techniques) before they are granted access to information, computers, and applications. Tightly manage and track physical access to devices.	SCS 9001 requires that organizations conduct a Security Risk Analysis which includes consideration of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure and limited access to such sensitive data to only those requiring such access to perform their job function. Multi-factor authentication can be implemented if required. All assets are tracked and enhanced policies such as data cleansing during repairs and/or end of life disposal of assets are required.
Protect sensitive data If your enterprise stores or transmits sensitive data, make sure that this data is protected by encryption both while it's stored on computers as well as when it's transmitted to other parties. Consider utilizing integrity checking to ensure only approved changes to the data have been made. Securely delete and/or destroy data when it's no longer needed or required for compliance purposes.	SCS 9001 requires that organizations protect sensitive data employing a NIST Federal Information Processing Standards-valid cryptography standard or equivalent when at rest (stored), in use (memory) and in transit (sent across networks). Cryptographic control policies for managing business encryption of assets and data are to be established, documented, and evaluated at least annually for effectiveness. SCS 9001 also details end of life disposition policies for the secure disposal of data.
Conduct regular backups Many operating systems have built-in backup capabilities; software and cloud solutions are also available that can automate the backup process. A good practice is to keep one frequently backed up set of data offline to protect it against ransomware.	SCS 9001 requires that organizations backup copies of information, software and system images and test those backups regularly in accordance with an established backup process. The process includes regularly performing and testing data backups, regularly performing complete, comprehensive, and resilient data backups, and protection of the confidentiality of backups at storage locations.
Protect your devices Consider installing host-based firewalls and other protections such as endpoint security products. Apply uniform configurations to devices and control changes to device configurations. Disable device services or features that are not necessary to support mission functions. Ensure that there is a policy and that devices are disposed of securely.	SCS 9001 requires that organizations protect all endpoint devices, local and remote. SCS 9001 requires that devices be hardened to enable only the necessary ports, protocols, and services to meet business needs and provide monitoring and technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template. Finally, SCS 9001 requires that all assets be properly handled upon end-of-life disposal including the removal of sensitive data.

Manage device vulnerabilities Regularly update both the operating system and applications that are installed on your computers and other devices to protect them from attack. If possible, enable automatic updates. Consider using software tools to scan devices for additional vulnerabilities; remediate vulnerabilities with high likelihood and/or impact.	SCS 9001 requires that organizations maintain all assets with the most recent updates and document the patch levels of all assets in the asset inventory database. Application of updates should follow the recommendations of the vendors of those assets. SCS 9001 requires that organizations apply vulnerability assessment and scanning tools or services to identify and resolve security vulnerabilities of organization's information systems. Further, the organization is required to apply additional measures such as the instrumentation and monitoring of all network boundaries and real-time scans of files from external sources as files are downloaded, opened, or executed.
Train users Regularly train and retrain all users to be sure that they are aware of enterprise cybersecurity policies and procedures and their specific roles and responsibilities as a condition of employment.	SCS 9001 requires that organizations determine the necessary competence of person(s) doing work under its control, ensures that these persons are competent on the basis of appropriate education, training, or experience, takes action to acquire necessary competence and retain evidence of such competence. Further, SCS 9001 requires annual Security Awareness Training for all employees, contractors, and 3rd party users with access to corporate assets.
DETECT Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. This Key Function identifies 4 activities.	
Test and update detection processes Develop and test processes and procedures for detecting unauthorized entities and actions on the networks and in the physical environment, including personnel activity. Staff should be aware of their roles and responsibilities for detection and related reporting both within your organization and to external governance and legal authorities	SCS 9001 requires that organizations instrument their networks and systems and log detection of anomalous behavior. Escalation processes are to be developed and tested following a formal process and identification of roles. SCS 9001 requires that organizations document procedures to detect technical vulnerabilities within organizationally owned or managed applications, infrastructure network and system components. Staff are to be trained as to their role and determined to be competent in those roles as part of an Incident Management Process.

Know the expected data flows for your enterprise If you know what and how data is expected to be used for your enterprise, you are much more likely to notice when the unexpected happens – and unexpected is never a good thing when it comes to cybersecurity. Unexpected data flows might include customer information being exported from an internal database and exiting the network. If you have contracted work to a cloud or managed service provider, discuss with them how they track data flows and report, including unexpected events.	SCS 9001 requires that organizations establish Security Policies within the appropriate business processes supporting confidentiality, integrity, and availability across system interfaces, jurisdictions, and business functions. Additionally, the organization is required to develop a network architecture through Secure Network and Systems Planning that includes network diagrams identifying high-risk environments and data flows that may have legal compliance impacts as well as limiting access to sensitive data.
Maintain and monitor logs Logs are crucial in order to identify anomalies in your enterprise's computers and applications. These logs record events such as changes to systems or accounts as well as the initiation of communication channels. Consider using software tools that can aggregate these logs and look for patterns or anomalies from expected network behavior.	SCS 9001 requires not only continuous network monitoring for anomalous behavior with a special focus at network boundaries, but also monitoring access control of all assets with logging. SCS 9001 requires that organizations deeply instrument their operations in areas such as monitoring asset access, creating logs of administrative actions, network traffic, and automated equipment identification be used as a method of connection authentication, amongst other requirements.
Understand the impact of cybersecurity events If a cybersecurity event is detected, your enterprise should work quickly and thoroughly to understand the breadth and depth of the impact. Seek help. Communicating information on the event with appropriate stakeholders will help keep you in good stead in terms of partners, oversight bodies, and others (potentially including investors) and improve policies and processes.	SCS 9001 requires that organizations conduct a number of self-assessments including Security Risk Analysis, Operational Risk, Technical Vulnerability Management and Supply Chain Risk Management. Findings are addressed and processes are reviewed and updated regularly for continuous improvement. Further, the organization is required to perform a Business Impact Assessment (BIA) that determines the key factors on protections of assets and networks. The BIA shall include External Provider Input and that the organization implement methods for collaboration with external providers on supply chain and security planning activities. Finally, SCS 9001 requires that organizations establish an Incident Management Policy, to be used during response to a cyber incident.

RESPOND Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. This Key Function identifies 3 activities.	
Ensure response plans are tested It's even more important to test response plans to make sure each person knows their responsibilities in executing the plan. The better prepared your organization is, the more effective the response is likely to be. This includes knowing any legal reporting requirements or required information sharing.	SCS 9001 requires organizations establish an Incident Management Process that is maintained as a documented operational incident response process for organizational systems, products, and services that includes preparation, detection, analysis, containment, recovery, and user or customer response activities. The process includes but is not limited to establishment and maintenance of a security incident response team(s) with a defined set of roles, responsibilities, competencies, and decision-making authority for each phase of the security incident management process and related activities, the implementation of a security information and event management system or its equivalent, to aggregate relevant data from multiple sources, identify deviations from the norm, and take appropriate action.
Ensure response plans are updated Testing the plan (and execution during an incident) inevitably will reveal needed improvements. Be sure to update response plans with lessons learned.	SCS 9001 requires that all operational and security processes be regularly evaluated for effectiveness and updated as appropriate with the goal of continuous improvement. SCS 9001 also requires that incident management plans be tested outside of an actual event to ensure processes function as expected and employees are trained in the execution of the response plan.
Coordinate with internal and external stakeholders It's important to make sure that your enterprise's response plans and updates include all key stakeholders and external service providers. They can contribute to improvements in planning and execution.	SCS 9001 requires that organizations establish effective Problem Resolution Processes which include documenting the event, resolution options such as immediate patching, source code corrections, deferring solutions to a planned release, and providing documented work-around(s) until a permanent resolution is provided. Further, requirements are to be established when corrective action is required of an external provider if determined that the external provider has culpability.

RECOVER Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event This Key Function identifies 3 activities.	
Communicate with internal and external stakeholders Part of recovery depends upon effective communication. Your recovery plans need to carefully account for what, how, and when information will be shared with various stakeholders so that all interested parties receive the information they need but no inappropriate information is shared.	SCS 9001 requires that all incidents be logged with supporting information and that an Incident Management Process be established for organizational systems, products, and services that includes preparation, detection, analysis, containment, recovery, and user / customer notification and response activities.
Ensure recovery plans are updated As with response plans, testing execution will improve employee and partner awareness and highlight areas for improvement. Be sure to update Recovery plans with lessons learned.	SCS 9001 requires that organizations assess their vulnerability with a Business Impact Analysis and implement plans for recovering from incidents with a Business Continuity Plan. Business Continuity Plans are to be tested and evaluated for effectiveness at least annually, and whenever there are significant organizational or environmental changes. Objective evidence of these activities shall be retained.
Manage public relations and company reputation One of the key aspects of recovery is managing the enterprise's reputation. When developing a recovery plan, consider how you will manage public relations so that your information sharing is accurate, complete, and timely – and not reactionary.	SCS 9001 requires that the organization implement a Business Continuity Plan, an element of which requires a notification process through which customers and other interested parties be updates for the extent and duration of any situation impacting customer operations. Further, through a required Incident Management Process, it is inferred which 3rd parties are to be notified of security incidents and the level of information to appropriately share depending on the party.

Conclusion

The U.S. government is demanding improvements in cybersecurity and supply chain risk management from the ICT industry. The U.S. BEAD program, through the directions provided in the NOFO, set unprecedented baseline requirements in specifying prudent cybersecurity and supply-chain risk management practices for States (Eligible Entities) which are to receive attestations from those deploying or upgrading broadband networks using BEAD funds (Subgrantees) to ensure compliance with stated expectations.

The NOFO requires that each Subgrantee have a plan that is operational prior to providing service that complies with:

- U.S. Executive Order 14028
- NIST Framework for Improving Critical Infrastructure Cybersecurity (the subject of this Tech Bulletin)
- NISTIR 8276 Key Practices in Cyber Supply Chain Risk Management: Observations from Industry
- NIST 800-161 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations as the requirements.

SCS 9001 is a Cyber and Supply Chain security standard which demonstrates the proper operational hygiene of vendors in delivering products and services to organizations who operate networks, be they private or public. SCS 9001 was developed in support of network operators in evaluating their suppliers and providing higher assurance that vendors:

- Operate their businesses with integrity and transparency
- Conduct all aspects of operations and product development with a high level of security
- Deliver products that are inherently higher in security and quality
- 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.

TIA has reviewed the BEAD NOFO baseline requirements and has confirmed that a certification to SCS 9001 will meet the requirements. Further, as SCS 9001 requires periodic recertifications, the standard is also useful in meeting the NOFO expectations that the Subgrantee plans be reevaluated and updated on a periodic basis and as events warrant.

Finally, and specific to the NIST Cybersecurity Framework, certification to SCS 9001 provides assurance that the certifying organization has achieved the goals of the Tier 4 Adaptive Implementation Tier.

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 Cybersecurity Framework (home page)

Cybersecurity Framework | NIST

- NIST Cybersecurity Framework Quick Start Guide – NIST Special Publication SP 1271

Getting Started with the NIST Cybersecurity Framework: A Quick Start Guide

- NIST Cybersecurity Framework V1.1 (full document)

Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (nist.gov)

- NIST Cybersecurity Framework V2.0 RFI Response Summary

NIST Cybersecurity RFI Summary Analysis

- 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)