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

Colin Black Andrews
Senior Director, Government Affairs

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

April 25, 2022

TABLE OF CONTENTS

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

I. Introduction and Summary

The Telecommunications Industry Association ("TIA") appreciates the opportunity to provide input to the National Institute of Standards and Technology ("NIST") on its Request for Information on *Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management* ("RFI").[1] TIA represents more than four hundred domestic and global manufacturers and vendors of telecommunications equipment and services. TIA's members manufacture and implement the equipment that composes secured networks across the country and keeps Americans connected with secure, high-speed networks. TIA is also an ANSI-accredited standards development organization and runs industry programs related to numbering, cabling technologies, smart buildings, quality, and supply chain security. As such, information and communications technology ("ICT") security is one of TIA's core focuses, and we welcome this opportunity to provide input to NIST on the critical work of updating the Cybersecurity Framework ("Framework" or "CSF").

[1] NIST Request for Information; 87 FR 9579, *Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management* (February 22, 2022).

TIA has been engaged with NIST on the development of the Framework since its inception and is pleased to see the immense success CSF V1.1 has had in just five years.[2] However, even with the Framework's widespread recognition among governments and organizations across many sectors, more work can and should be done to encourage its use – and help advance supply chain risk management ("SCRM") more generally – throughout the marketplace. NIST can support this effort by leveraging its new National Initiative for Improving Cybersecurity in Supply Chains ("NIICS") to drive awareness and education among organizational decision-makers about the importance of SCRM, the use of the CSF, and how to prioritize cyber and supply chain risk management in a cost-effective manner.

As NIST considers potential updates to the Framework itself, it should remember that the Framework as it exists has been widely successful and should not seek to materially change the Framework Core. For example, many government dockets are contemplating including requirements on industry regarding governance and third-party risk. TIA believes that NIST should not include additional Functions on "Governance" and "Supply Chain/Dependency Management" at this time. As Framework users continue to advance risk management practices, they can choose to incorporate these Functions in their sector or organizational CSF Profiles. Should these Functions gain traction across a more widespread set of CSF users, NIST may reconsider whether to incorporate these Functions into the Framework Core.

[2] *See, e.g.*, TIA Comments on NIST Request for Information, *Views on the Framework for Improving Critical Infrastructure Cybersecurity*, Doc. No. 151103999-5999-01 (Feb. 23, 2016) (*available at* https://tiaonline.org/wp-content/uploads/2018/02/TIA-Comments_NIST-RFI_FrameworkViews_Final.pdf; TIA Comments on NIST Request for Comment *Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity*, Doc. No 130208119-3119-01 (Apr. 10, 2017) (*available at* https://tiaonline.org/wp-content/uploads/2018/02/TIA-Comments-on-NIST-Framework-Update-4-10-2017.pdf), TIA Comments on NIST Request for Comment on *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 Draft 2*, (Jan. 19, 2018) (*available at* https://tiaonline.org/wp-content/uploads/2018/02/TIA-Comments-on-CSF-V1.1-Draft-2_.pdf).

TIA agrees with the RFI that NIST should actively work to harmonize the CSF with related NIST tools published since the release of CSF V1.1. NIST should also incorporate additional industry resources, that align with the CSF and advance NIST's goals, including TIA's SCS 9001: Supply Chain Security Standard ("SCS 9001"). Similarly, TIA supports further integration of the Framework and cybersecurity supply chain risk management guidance. However, NIST need not undergo drastic changes to the Core itself to do so. NIST can accomplish this goal by including more SCRM-specific touchstones, such as SCS 9001, among others, within the CSF Informative References.

Finally, TIA supports NIST working with the National Telecommunications and Information Administration ("NTIA") as they fund broadband networks nationwide through the Infrastructure Investment and Jobs Act's Broadband Equity, Access, and Deployment ("BEAD") Program and utilize the revised framework to meet NTIA's cybersecurity and supply chain security goals for the program.

We again thank NIST for the opportunity to elaborate on these points below and welcome further discussion as NIST works on this important effort to update the Framework.

II. NIST's NIICS Should Broadly Promote Awareness and Understanding of SCRM Among Organizational Decisionmakers.

The RFI seeks input on both challenges that may prevent organizations from using the Framework and challenges related to the cybersecurity aspects of SCRM more broadly. Even as more organizations recognize cybersecurity as a business imperative, leaders in many organizations still view cybersecurity as a cost center and/or lack awareness about how to cost-effectively prioritize and address SCRM within their organization's missions.[3] This tendency

[3] *See* Gartner, 6 Key Takeaways from the Gartner Board of Directors Survey (Oct. 21, 2021), https://www.gartner.com/en/articles/6-key-takeaways-from-the-gartner-board-of-directors-survey (which found that the percentage of boards who consider cybersecurity as a business risk as opposed to an IT problem rose from 58%

can be seen across organizations of all sizes, but particularly within small and medium-sized entities.[4]

The NIICS can help address these challenges by: (1) driving awareness and education among organizational decisionmakers about the imperative value of SCRM to businesses and organizations of all types; (2) building understanding among organizational leaders about how to maximize SCRM investments (including through use of the Framework); and (3) coordinating with complementary federal initiatives to drive such education and awareness throughout the NIICS program.

i. Drive awareness about SCRM as an organizational imperative.

The NIICS should focus on enhancing SCRM through strategic outreach to organizational leadership, emphasizing not only SCRM's importance from an organizational perspective but also developing/promoting actionable steps organizations of all sizes and across multiple sectors can take to incorporate SCRM practices in their organizations in a cost-effective manner. As part of this awareness campaign, NIICS should encourage use of the Framework as a flexible, adaptable tool to accomplish an organization's risk management goals in a manner that is tailored to meet its unique needs.[5]

---

to 88% in the last five years). *See also* PwC, Can the CEO make a difference to your organisation's cybersecurity?, https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights/ceos-in-cyber.html (which found that 37% of CEOs surveyed said they provide significant support for "ensuring adequate resources, funding, and sufficient priority" to cyber teams. Only 30% of non-CEO executives agreed that their CEO does so.); Brian Eastwood, Security strategies evolve while spending flatlines, Cybersecurity Dive (Feb. 8, 2022), https://www.cybersecuritydive.com/news/security-technology-budget-2022/618434/.

[4] USTelecom, USTelecom 2021 Cybersecurity Survey – Critical Infrastructure Small & Medium-Sized Businesses (SMBs) (2021), https://www.ustelecom.org/wp-content/uploads/2021/03/USTelecom-2021-Cyber-Survey.pdf.

[5] NIST, Cybersecurity Framework – Getting Started, https://www.nist.gov/cyberframework/getting-started (last visited Apr. 19, 2022); NIST, Cybersecurity Framework – Success Stories, https://www.nist.gov/cyberframework/success-stories (last visited Apr. 19, 2022).

The NIICS will benefit from the running start provided by the numerous online learning materials NIST already makes publicly available. For example, the Framework's Quick Start Guide points to some actionable, cost-effective steps an organization can take to achieve the Framework's key Functions (Identify, Protect, Detect, Respond, Recover). The Guide highlights activities such as tracking hardware and software inventory as part of the Framework's "Identify" key Function, and the ability to do so with a simple spreadsheet.[6] Building awareness about these tools can help demonstrate to organizations how easy it is to use the Framework to manage and communicate risk.

Through dialogue with organizational leaders, NIICS can also encourage Framework adoption by identifying additional areas that are ripe for Profile development. NIST's work with specific stakeholder groups to develop Profiles – such as those for the financial sector,[7] for Positioning, Navigation, and Timing ("PNT") services,[8] for the manufacturing industry,[9] and in various other use cases[10] – helps to simplify use for organizations new to the Framework and foster collaboration and consistency across similarly situated organizations. Developing additional Profiles, based on current input from a wider range of organizational leaders, can help

[6] NIST, Computer Security Resource Center – Cybersecurity Framework, Getting Started with the NIST Cybersecurity Framework: A Quick Start Guide, https://csrc.nist.gov/Projects/cybersecurity-framework/nist-cybersecurity-framework-a-quick-start-guide (last visited Apr. 19, 2022).

[7] Cyber Risk Institute, The Profile is the benchmark for cyber risk assessment, https://cyberriskinstitute.org/the-profile/ (last visited Apr. 19, 2022).

[8] Michael Bartock, et al., *Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services (NISTIR 8323)*, National Institute of Standards and Technology (Feb. 2021), https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8323.pdf.

[9] Keith Stouffer, et al., Cybersecurity Framework Version 1.1 Manufacturing Profile (NISTIR 8183, Rev. 1), National Institute of Standards and Technology (Oct. 2020), https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8183r1.pdf.

[10] NIST, Cybersecurity Framework – Examples of Framework Profiles, https://www.nist.gov/cyberframework/examples-framework-profiles (last visited Apr. 19, 2022).

address SCRM gaps in the ecosystem and enlist a broader set of stakeholders in the success of the Framework in support of our collective SCRM goals.

ii. Build understanding of how to maximize SCRM investment.

A critical part of this education/awareness effort will be giving organizations an actionable understanding of how they can maximize their investments in SCRM. As the Framework itself appreciates, organizational leaders constantly face tradeoffs in determining how to allocate an organization's resources. Effective SCRM relies on concrete determinations of what risk management investments pay the most dividends – recognizing that such dividends can vary based on the risk context.

The NIICS can help reduce the burden on organizations making these determinations by working with stakeholders to identify key actions that maximize investments in SCRM. This may include activities like evaluating the cost-effectiveness of various controls included in the Framework itself based on common use cases. While the ideas NIST provides in its Quick Start Guide to implementing the Framework provide a window into how the Framework's Functions could be implemented (as demonstrated in the spreadsheet example mentioned above), a more comprehensive evaluation of how controls in each of the Framework's categories can impact the overall risk posture of an organization can provide tangible information for decisionmakers to weigh the relative benefits of risk management activities and justify these investments to other stakeholders throughout the organization. NIST should focus such cost-effectiveness evaluation on categories or use cases that apply to the largest possible set of organizations (to maximize awareness and adoption) and could consider sharing the methodology for conducting these evaluations with stakeholders for their own use as well.

iii. Coordinate with complementary federal initiatives to reach key stakeholders.

Agencies across the federal government are simultaneously pursuing initiatives to drive education and awareness about cybersecurity and supply chain risk management. As NIST develops the NIICS, it should pursue opportunities to leverage existing initiatives to maximize its reach to stakeholders and contribute to harmonized government messaging about cybersecurity and SCRM. For example, NTIA's Communications Supply Chain Risk Information Partnership ("C-SCRIP") is committed to improving equipment suppliers' and rural and small communications providers' access to information about risks to key supply chain elements.[11] Given its similar mission, C-SCRIP can help the NIICS reach leaders in small and medium-sized ICT organizations, which would particularly benefit from use of the Framework and whose enhanced SCRM practices would in turn benefit the broader connected ecosystem.[12]

The NIICS and C-SCRIP could likewise leverage the landmark work of the Federal Communications Commission's ("FCC's") fourth iteration of the Communications Security Reliability and Interoperability Council ("CSRIC IV"), which developed guidance for each of the five communications sector segments (Wireline, Wireless, Cable, Broadcast, and Satellite) to implement the Framework.[13] Similarly, groups like the Department of Homeland Security's ("DHS's") ICT SCRM Task Force continue to develop guidance to help enhance SCRM.[14] The

[11] NTIA, NTIA's Communications Supply Chain Risk Information Partnership (C-SCRIP), https://www.ntia.doc.gov/cscrip (last visited Apr. 19, 2022).

[12] USTelecom, USTelecom 2021 Cybersecurity Survey – Critical Infrastructure Small & Medium-Sized Businesses (SMBs) (2021), https://www.ustelecom.org/wp-content/uploads/2021/03/USTelecom-2021-Cyber-Survey.pdf. (explaining that an SMB failure "can impact the broader digital ecosystem leading to financial and reputational loss and service disruption," making "understanding the organizational behavior of companies of various sizes" imperative).

[13] The Communications Security, Reliability and Interoperability Council IV, Cybersecurity Risk Management and Best Practices Working Group 4: Final Report (Mar. 2015), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

[14] Cybersecurity & Infrastructure Security Agency, Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force, https://www.cisa.gov/ict-scrm-task-force (last visited Apr. 19, 2022).

NIICS can profoundly benefit the security and resiliency of the connected ecosystem by bringing these tools together and sharing them directly with organizational decisionmakers in tangible, actionable ways.

III. NIST Should Not Include "Governance" and "Supply Chain/Dependency Management" as Individual Functions at this Stage.

NIST staff have posed questions about whether to follow the financial sector's lead and include "governance" and "supply chain/dependency management" as additional Functions in the Framework update.[15] Meanwhile, the Securities and Exchange Commission ("SEC") has included similar considerations in its proposed rule on heightened cyber incident disclosures for public companies.[16]

NIST should refrain, at least for the time being, from adopting proposals that originated in the financial sector. Although NIST's inclusion of these additional Functions in the Framework update ostensibly could help align understanding across federal agencies and public companies about what these practices should look like, they are not necessarily applicable or appropriate outside the financial sector. Indeed, these Functions as articulated in the financial sector's Profile are designed to directly respond to regulatory expectations specific to that sector; they are not ripe for application to the Framework's broader set of users, including in particular the IT and communications sectors.

Moreover, governance and third-party risk are already included within the existing Framework to some degree. Because the Framework is a stakeholder-driven tool and developed

[15] Cyber Risk Institute, The Profile is the benchmark for cyber risk assessment, https://cyberriskinstitute.org/the-profile/ (last visited Apr. 19, 2022).

[16] Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies, 87 Fed. Reg. 13524 (Mar. 9, 2022), https://www.federalregister.gov/documents/2022/03/09/2022-03145/cybersecurity-risk-management-for-investment-advisers-registered-investment-companies-and-business.

for use by stakeholders, NIST should wait to see if users adopt those Functions organically before expanding the Framework currently in use. The SEC's proposed rule on heightened cyber disclosure is already exploring these issues, and NIST should wait to see how stakeholders weigh in on these issues throughout the SEC process. Ultimately, NIST can have more impact on these points by proactively engaging in the NIICS awareness/education initiative described above, as expanding the list of the Framework's Functions could potentially only further deter organization leaders from Framework adoption by making it seem more onerous and less cost-effective to implement.

IV. NIST Should Harmonize the Framework with Related Tools.

Since its initial publication in 2016, the Framework has become a foundational tool for communicating cybersecurity risk management across disparate professional disciplines, organizations, sectors, and international borders. The success of the Framework has heightened widespread awareness of the technical expertise and unique convening capabilities of NIST itself – and NIST has become the go-to forum for public-private collaboration to develop influential guidance addressing some of our most pressing challenges. Organizations – both public and private – increasingly look to tools such as the Privacy Framework and the Secure Software Development Framework to identify, manage, and communicate their organizational or product risk posture and how it operates within its environment. The AI Risk Management Framework, currently under development, will also have important intersections with the CSF.

NIST can and should explore harmonization among its tools as it considers updates to the CSF in response to this RFI, but harmonization should also be an ongoing effort as thinking across these areas of guidance continues to progress. Additionally, as an expert in the security realm and as a convener of public private partnerships, NIST should stay apprised of other

government efforts focused on ICT security to ensure there is not overlap with existing workstreams. NIST should also incorporate additional industry tools as Informative References to help users understand how the standards and certifications that they use can support their alignment with the Framework itself. This should include industry-led standards like SCS 9001, which – like the Framework – address organizational risk management, and which align with related NIST guidance.

V. NIST Should Further Integrate Supply Chain Risk Management into the Framework by Including SCS 9001 as an Informative Reference.

Over the last six years, TIA and its members have worked in close partnership with the U.S. government to build awareness and understanding of supply chain threats and enhance the security of the global ICT ecosystem. TIA works to advance these efforts as an ANSI-accredited standards body and through service in leadership positions on the IT and Communications Sector Coordinating Councils and on DHS's ICT Supply Chain Risk Management Task Force, as well as membership on the FCC's CSRIC.

TIA is working directly to enhance SCRM through development of the SCS 9001 standard focused on supply chain security and its benchmarking and third-party certification program. After its acquisition of QuEST Forum in 2017, TIA set to work leveraging its unique quality management system capabilities to develop SCS 9001, a process-based standard that provides comprehensive supply chain assurance benchmarked across the ICT marketplace. SCS 9001 verifies trust across 10 security domains with 54 controls, and seven additional processes with requirements that support key policy priorities such as software bill of materials, zero trust architecture, supplier trust principles, incident management and response, among others. In addition to verifying that a product is built on a sound foundation of trust, SCS 9001 can also help illuminate suppliers of concern within the supply chain.

SCS 9001 is third-party certified, leveraging an existing global network of accreditation bodies and certification bodies to enable organizations to implement, measure, and improve their supply chain processes. SCS 9001 was built after extensively reviewing existing standards and ICT SCRM best practices, including NIST SP 800-161. It aligns with the Prague Proposals,[17] and goes beyond ISO 9001 and ISO 27001 where appropriate to support the demanding needs of ICT and evolving security priorities.[18] SCS 9001's benchmarking process can help illuminate SCRM performance, drive competitive improvement (rather than backward compliance), and provide assurance to government as well as private sector customers without compromising the privacy, security, or intellectual property of suppliers undergoing certification.

SCS 9001 can also help to harmonize existing cyber and supply chain workstreams currently underway in the Administration. For instance, TIA has mapped out how SCS 9001 is aligned with Executive Order 14028 *Improving the Nation's Cybersecurity*,[19] and how utilization of SCS 9001 could help the Administration achieve the goals of this EO. EO 14028 is split into ten sections aimed at improving the country's cybersecurity and ways the government can cooperate with industry resiliency and remediate cyber incidents. SCS 9001 supports all ten sections of this EO. For instance, utilizing the standard can fulfill Section 2's goal of removing barriers to sharing threat information by creating technical vulnerability management to evaluate

[17] TIA, How TIA QuEST Forum's SCS 9001 Supply Chain Security Standard Aligns with the Prague Proposals, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/viewer.html?pdfurl=https%3A%2F%2Ftiaonline.org%2Fwp-content%2Fuploads%2F2022%2F03%2FPrague-Proposals-vs-SCS-9001-Final-021522.pdf&clen=219327&chunk=true (last visited Apr. 25, 2022).

[18] TIA, SCS 9001: Why ICT Security Must Go Beyond ISO 27001, https://tiaonline.org/scs-9001-why-ict-security-must-go-beyond-iso-27001/ (last visited Apr. 25, 2022).

[19] Executive Order 14028 of May 12, 2021, *Improving the Nation's Cybersecurity*, 86 FR 26633 (*available at* https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity.

and report on security vulnerabilities, and establishing an incident management process to ensure cyber incidents are mitigated as quickly as possible.

TIA would welcome the opportunity to brief NIST staff on SCS 9001 and how this standard maps to ongoing government requirements for both cybersecurity and 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 incorporation of SCS 9001 as an Informative Reference can help users understand how to align their SCRM practices within the Framework.

VI. NIST Should Collaborate with NTIA to Leverage the Framework to Fulfill Cybersecurity and Supply Chain Directives in the BEAD Program.

Division F of the Infrastructure Investment and Jobs Act tasks NTIA with establishing the BEAD Program to drive equitable access to broadband throughout the United States. As part of this program, the statute (1) directs NTIA to "provide technical and other assistance to eligible entities regarding cybersecurity resources and programs available through federal agencies," including the Cybersecurity and Infrastructure Security Agency ("CISA") and NIST,[20] and (2) requires grant recipients to "comply with prudent cybersecurity and supply chain risk management practices" as specified by NTIA in consultation with NIST and the FCC.[21]

NTIA can and should fulfill both directives by instructing grant applicants to demonstrate that their cybersecurity and supply chain practices align with the Framework. This approach would provide applicants with ready-to-use guidance that is consistent and technologically neutral, and afford accountability, transparency, and predictability to states and the federal government regarding how federally funded networks are being protected. Moreover, it would

[20] 47 U.S.C. § 1702(b)(4)(B)(ii).

[21] 47 U.S.C. § 1702(g)(1)(B).

ensure future-proof implementation of the BEAD cybersecurity and supply chain requirements, as the Framework provides the foundation for an adaptive, assurance-based process that NIST and its stakeholders can update over time.

VII. Conclusion

TIA appreciates the opportunity to provide initial input in response to NIST's RFI. The Framework has become an important tool for communicating risk management across the widespread and diverse value chains in our increasingly connected world. The NIICS can promote use of the Framework – and SCRM more broadly – by building targeted education and awareness among organizational leaders. As NIST considers updates to the Framework, it should not seek to substantially modify the Framework, but rather continue to harmonize the CSF with other NIST and industry tools. By incorporating TIA's SCS 9001 as an Informative Reference, NIST can further integrate SCRM considerations into the Framework and provide more concrete guidance to Framework users on how to build SCRM into their organizational practices.

TIA looks forward to continued partnership with NIST as it 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

April 25, 2022