BEFORE THE
DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
WASHINGTON, D.C. 20554

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

COMMENTS OF NCTA – THE INTERNET & TELEVISION ASSOCIATION

Matthew J. Tooley
Vice President, Broadband Technology
Science & Technology

Rick Chessen
Loretta Polk
Becky Tangren
NCTA – The Internet and Television Association
25 Massachusetts Ave., N.W. – Suite 100
Washington, DC 20001-1431
(202) 222-2445

April 25, 2022

CONTENTS

BEFORE THE
DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
WASHINGTON, D.C. 20554

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

COMMENTS OF NCTA – THE INTERNET & TELEVISION ASSOCIATION

NCTA - The Internet & Television Association ("NCTA") hereby responds to the above-captioned Request for Information ("RFI") released by the National Institute of Standards and Technology ("NIST"), in which NIST seeks public input on updating its *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1* ("Cybersecurity Framework" or "Framework").[1]

I. INTRODUCTION AND SUMMARY

The Cybersecurity Framework has been a tremendously successful tool for evaluating and managing cybersecurity risk by organizations large and small. Its success results from NIST's collaborative approach to development and implementation of the Framework, driven by technical expertise and bolstered by NIST's receptiveness to stakeholder input and recommendations. This nearly decade-long public-private collaborative process, led by NIST

[1] *Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management*, Notice of Inquiry, 87 FR 9579, Nat'l Inst. of Standards and Tech. ("NIST") (Feb. 22, 2022) ("RFI"); Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, NIST, (Apr. 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf ("Cybersecurity Framework").

and including robust participation from NCTA and its member companies, has resulted in a key resource for domestic and international organizations – including cable operators. The Framework serves as a compendium for dynamic and effective cybersecurity risk management, and as a guidepost for gauging cyber readiness, and strengthening cybersecurity practices and processes.

Many public and private organizations have used the Cybersecurity Framework as a foundation for their cybersecurity risk management activities. This is because it is scalable, adaptable, and technology- and threat-agnostic.[2] It is not a compliance checklist. As NIST has previously explained, "[t]here are no 'silver bullets' when it comes to cybersecurity and protecting an organization."[3] Accordingly, a framework that can be tailored for a particular organization or cybersecurity risk profile has the potential to promote more wide-scale adoption across various sectors.

Given that Version 1.1 of the Framework is now about four years old, NCTA agrees that targeted updates could help promote broader adoption and make the Framework even more useful and effective. As NIST moves forward, however, its overriding priority should be to continue to advance and promote the dynamic, flexible, scalable, and adaptable approach embodied in the Framework to date and encourage broader adoption by clarifying its applicability across all sectors, including with respect to supply chain and IoT security issues. NIST can also ensure continuity between enterprises' implementation of previous and revised versions, and avoid conflicting with or undermining previous versions, by making any updates backwards compatible. The emphasis of this effort should be on targeted modernization and

[2] *See, e.g., id.*

[3] Cybersecurity Framework: Questions and Answers, NIST (Feb. 24, 2022), https://www.nist.gov/cyberframework/frequently-asked-questions/framework-basics#basics.

rationalization of the Framework to account for changing circumstances and gaps in adoption to date, rather than rethinking the Framework's fundamental approach or trying to tailor the Framework to any incompatible uses such as prescriptive compliance rules.

II. THE CABLE INDUSTRY HAS SUCCESSFULLY IMPLEMENTED THE CYBERSECURITY FRAMEWORK.

Cybersecurity is of central importance to the entire communications ecosystem. And for cable providers, in particular, it is a core business imperative. NCTA's members provide the majority of residential and commercial broadband services in the U.S. To grow and maintain their customer relationships, our members must deliver broadband services that are reliable and products that keep their customers safe and secure online, so they have strong incentives to maintain secure, reliable networks. This is evidenced by their extensive investments in security features and contributions to the ongoing development of industry standards and best practices.[4]

Consistent with those incentives, for many years NCTA's members have made considerable efforts and devoted significant resources towards developing and promoting effective cybersecurity solutions. For example, the cable industry's long-standing and globally recognized Data Over Cable Service Interface Specifications ("DOCSIS"), a globally-recognized standard, has incorporated security from its inception.[5] Individual cable operators, including Comcast, Charter Communications, and Cox Communications, continually seek to improve their cybersecurity programs and provide their customers with significant resources to arm them with the tools necessary to combat cybersecurity threats. For example, Charter offers its customers a managed security service that contains a managed firewall with VPN and a unified threat

[4] Gateway Device Security Best Common Practices, CableLabs (Oct. 2021), https://www.cablelabs.com/specifications/CL-GL-GDS-BCP.

[5] *See* DOCSIS 4.0 Technology, CableLabs, https://www.cablelabs.com/technologies/docsis-4-0-technology (last accessed Apr. 25, 2022).

management system.[6] Likewise, Cox offers a range of cybersecurity solutions that include WiFi encryption,[7] and Comcast has developed a tool called xGitGuard that scans GitHub repositories to identify if developers are hardcoding secrets, which goes against good security practices.[8]

A major component of cable operators' efforts to improve cybersecurity include working closely with NIST and other stakeholders to identify, establish, and implement industry best practices. For example, NCTA members contributed to the development of the Cybersecurity Framework. Most prominently, the cable sector was instrumental in leading the Communications Security, Reliability, and Interoperability Council's ("CSRIC") landmark effort in 2014-2015 to develop in-depth guidance for communications companies of all types to implement the Framework.[9] NCTA members were among the more than 100 cybersecurity experts who spent over a year developing 400 pages of implementation guidance tailored specifically for operators of cable, wireless, wireline, satellite, and broadcast networks. NCTA members adopted various cybersecurity and secure internet routing procedures from their work in CSRIC IV, Working Group 6, including traffic filtering at the border of stub networks and features like unicast Reverse Path Filtering on transit segments of their networks. [10] Together, these steps represented one of the most in-depth and rigorous effort to implement the Framework in any critical infrastructure sector.

[6] Managed Security Service, Spectrum Enterprise, https://enterprise.spectrum.com/services/internet-networking/managed-network/managed-security.html (last accessed Apr. 25, 2022).

[7] Cybersecurity Solutions, Cox, https://www.cox.com/residential/internet/learn/cybersecurity-options.html (last accessed Apr. 25, 2022).

[8] Comcast/xGitGuard, Comcast, https://github.com/Comcast/xGitGuard (last accessed Apr. 25, 2022).

[9] John Schanz of NCTA member Comcast was the Chair of CSRIC IV, and experts from other NCTA members provided significant time and resources to develop this report. *See* Cybersecurity Risk Management and Best Practices, CSRIC (Mar. 2015), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

[10] Secure BGP Deployment Final Report, CSRIC III, Working Group 6 17, 19-20 (Mar. 2015), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf; *see also* Comments of NCTA – The Internet & Television Association, In the Matter of Secure Routing, PS. Docket, No. 22-90, Federal Communications Commission (Apr. 2022), https://www.fcc.gov/ecfs/search/search-filings/filing/104121093502606.

Consistent with input to NIST in the collaborative development of the Framework, NCTA's members were already applying and using most, if not all, of the security functions that form the Core of the Framework prior to its public release in 2014.[11] Since 2014, however, our member companies have used the Framework to identify gaps in existing cybersecurity programs and implement structural changes to ensure comprehensive, risk-based cybersecurity programs are in place to address constantly-changing and pervasive cyber threats. The Framework helped to improve how our members performed third party risk assessments. The assessments have become more detailed both in terms of depth and breadth. In addition, the use of the Framework by our members has resulted in a corporate cultural shift in how cable operators view security. This cultural shift has resulted in a security by design mindset across the cable industry.

NCTA members have continued to innovate in cybersecurity and engage with other stakeholders in the public and private sectors across multiple technology areas, such as with respect to the Internet of Things ("IoT").[12] For example, NCTA members are part of the Open Connectivity Foundation ("OCF"),[13] an organization whose mission is to lead the development and deployment of a common, secure communications framework for IoT devices, and contributed to the development of the OCF Security Specification.[14] Cable operators also contributed to the C2 Consensus on IoT Device Security Baseline Capabilities[15] that resulted in

[11] *See* Cybersecurity Risk Management and Best Practices Working Group 4: Final Report, Communications Security, Reliability, and Interoperability Council ("CSRIC") IV, 25 (Mar. 2015), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

[12] *See* CableLabs Micronets, CableLabs, https://www.cablelabs.com/technologies/micronets (last accessed Apr. 25, 2022).

[13] OCF Security Specification, Open Connectivity Foundation ("OCF") (Jan. 2022), https://openconnectivity.org/specs/OCF_Security_Specification_v2.2.5.pdf.

[14] *See* About Open Connectivity Foundation, OCF, https://openconnectivity.org/foundation/ (last accessed Apr. 25, 2022).

[15] The C2 Consensus on IoT Device Security Baseline Capabilities, Council to Secure the Digital Economy, https://csde.org/wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf (last accessed Apr. 25, 2022).

the Consumer Technology Association's Baseline Cybersecurity for Devices and Device Systems (ANSI/CTA-2088).[16]

In accordance with its purpose and design, the Framework has proven scalable and adaptable – its risk-based approach to cybersecurity has allowed a diverse and growing variety of organizations to implement cybersecurity programs tailored to the particular risk tolerance, network architecture, customer environment, and institutional resources appropriate to that organization. The Framework in its current form promotes a holistic approach to cybersecurity. And it has reinforced existing marketplace incentives and raised the visibility of cybersecurity programs within NCTA member organizations to the C-suite, as a strategic risk management issue.

III. TARGETED UPDATES TO THE FRAMEWORK'S TIERS, PROFILES, AND OTHER ASPECTS WOULD BE VALUABLE IN HELPING ADVANCE EFFECTIVE FRAMEWORK IMPLEMENTATION.

The Cybersecurity Framework is comprised of: the Framework Core (desired cybersecurity activities and outcomes), the Framework Implementation Tiers (the degree to which an organization's cyber management practices exhibit the characteristics defined in the Framework), and the Framework Profiles (an organization's unique alignment to its desired outcomes with respect to the Core), as well as an Appendix of Informative References.[17] This structure intentionally allows the Framework to remain relatively unencumbered by sector- or technology-specific elements, including any "maturity model" traps that could calcify into rigid prescriptive compliance requirements. This design choice has been crucial for imbuing the

[16] Baseline Cybersecurity Standard for Devices and Device Systems (ANSI/CTA-2088), Consumer Technology Association (Dec. 2020), https://shop.cta.tech/collections/standards/products/baseline-cybersecurity-standard-for-devices-and-device-systems-cta-2088.

[17] *See* An Introduction to the Components of the Framework, NIST, https://www.nist.gov/cyberframework/online-learning/components-framework (last accessed Apr. 25, 2022).

Framework with the principle of proactive – indeed, *always* active – risk management – rather than reactive checklist compliance. This is an important part of what has made the Framework so successful, and NIST should avoid any updates or revisions that alter the Framework's fundamental nature.

Instead, NIST should focus on targeted updates that aim to modernize the Framework. For example, the Framework lacks clarity about its applicability across industries, particularly with respect to supply chain software and device manufacturers. NIST can make some small, but impactful, modifications that would clarify and expand the use of the Cybersecurity Framework without undermining its key strengths.

A. NIST Should Clarify The Role Of Tiers In Assessing Suppliers And Supply Chain Management Issues, and Reiterate That Tiers Are Not For Use as a Maturity Model.

The Framework Implementation Tiers ("Tiers") – Partial, Risk Informative, Repeatable, and Adaptive – are intended to contextualize cybersecurity risks and assist organizations in managing risk consistent with risk tolerance, resources, and other factors. The Tiers are designed to identify which aspects of an entity's organization pose a higher priority cybersecurity risk so that organizations can allocate additional resources to appropriately address that risk.[18] The Tiers approach has some utility and can be further improved with some targeted refinement, but NIST should continue to be mindful of the risk that the Tiers may be used by some as a maturity model.

NCTA has been clear in its concern that the Tiers approach risks becoming "little more than a rudimentary quantitative ranking scheme."[19] NIST helpfully responded to this concern by

[18] Cybersecurity Framework, at 9-11.

[19] Comments of NCTA – The Internet & Television Association, In the Matter of Experience with the Framework for Improving Critical Infrastructure Cybersecurity, Docket No. 140721609-4609-01, at 14 (2014).

stating unequivocally that the "Tiers do not represent maturity levels."[20] Instead, each Tier is intended to represent a target level of sophistication that can be effectively achieved by an organization to adequately address particular cybersecurity risks. Organizations determine their desired tier based on their own risk management practices, risk preferences, legal and regulatory requirements, cybersecurity risks, consumer needs, and other considerations.[21]

NCTA reiterates that the Tiers approach risks introducing antiquated maturity model concepts into a rapidly evolving technology and threat landscape. Nevertheless, we also recognize that the Tiers system as set forth in the Framework when used as NIST intended – as a mechanism for organizations to achieve their cybersecurity goals – can be an effective self-assessment tool because the descriptions of each Tier are broad and general, which allows a wide range of organizations to assess tailored aspects of their cybersecurity risk management programs. To that end, NCTA believes that the Tiers can be further enhanced with some minor revisions.

In particular, two areas where cable operators have found Tiers helpful are with supplier oversight and supply chain risk management issues. Using Tiers makes it easier to understand suppliers' approach to cybersecurity and supply chain risk management, which makes the cable network as a whole more secure. Organizations can leverage the Tiers system to better understand the cybersecurity posture of their suppliers, such as by analyzing their suppliers' cybersecurity risk management programs based on the guidance of the Tier descriptions to ensure that the organizations' suppliers maintain an adequate level of cybersecurity. Organizations can also use the Tiers to establish preferences based on suppliers' adherence to specific Tiers with respect to cybersecurity risk management for their organizations. However,

[20] Cybersecurity Framework, at 8.
[21] *Id.*

organizations have run into challenges with certain suppliers that have not implemented or assessed their systems based on the NIST Cybersecurity Framework because these suppliers do not believe that it applies or can be applied to them. NIST could help to resolve those challenges and expound upon the different ways that this system can be useful in the context of supply chain and supplier management issues.

B. The Framework Can Expand the Use of Profiles To Additional Use Cases.

The Profiles construct is another aspect of the Framework that has helped industry assess, develop, and implement cybersecurity measures and protocols. NIST has developed profiles that organizations can use to review aspects of their cybersecurity programs based on the elements and security objectives of the Framework.[22] Organizations can compare their cybersecurity programs with target Profiles to create a plan to improve their cybersecurity practices.

In refining the Cybersecurity Framework, NIST should describe how organizations can use Profiles and NIST's guiding principles of secure authentication, identity and access management to create desired targeted outcomes for different use cases, notably in supply chain security, IoT security, secure software development, and other issues relevant to various sectors. Explicit incorporation of these subtopics through the development of appropriate Profiles would help organizations address cybersecurity risks not currently included in the Cybersecurity Framework, increase harmonization across industries with respect to evolving cybersecurity threats, and address the gaps in adoption that hinder the Framework's utility and effectiveness across the internet ecosystem.

[22] *See e.g.*, NISTIR 8183 Revision 1 Cybersecurity Framework Version 1.1 Manufacturing Profile, NIST (Oct. 2020), https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8183r1.pdf; *see also* NISTIR 8374 Ransomware Risk Management: A Cybersecurity Framework Profile, NIST (Feb. 2022), https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8374.pdf.

C. The Framework Should Clarify How Organizations Can Develop Performance Goals for Their Cybersecurity Programs.

The Framework should also include a discussion on how it can be used to identify and develop consistent cybersecurity performance goals. In particular, NIST should include an explanation of how organizations develop performance goals tied to targeted outcomes of their Framework Profile. Without information about how to identify and develop performance goals, a variety of inconsistent or possibly conflicting performance goals may emerge and create confusion, and organizations have little guidance in assessing whether their implementation of the Framework is achieving their desired outcome.

NIST can bolster the Framework's reliability and effectiveness and ensure widespread adoption if it makes targeted clarifications and updates to encapsulate the entire internet ecosystem, including supply chain, IoT, software and other developers. Additionally, more broadly applicable cybersecurity performance goals – most prominently, those being developed by the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency ("CISA")[23] – should be developed specifically to align with the Cybersecurity Framework, rather than the reverse. NIST's focus should remain on continuing to refine and modernize the Framework to promote performance that allows organizations to reach any applicable performance goals that align with the Framework's robust approach to proactive risk management, rather than reverse engineering the Framework to any prescriptive goals that are incompatible with its dynamic, adaptive approach. Continued alignment of performance goals like those being developed by CISA with the Cybersecurity Framework bolsters both the

[23] Critical Infrastructure Control Systems Cybersecurity Performance Goals and Objectives, Cybersecurity and Infrastructure Security Agency ("CISA") (Sept. 21, 2021), https://www.cisa.gov/control-systems-goals-and-objectives.

performance goals and the Cybersecurity Framework, and promotes clarity and certainty of cybersecurity best practices across federal policy and private sectors.

IV. NIST SHOULD LEVERAGE ITS NATIONAL ONLINE INFORMATIVE REFERENCES PROGRAM TO ALIGN ITS BROADER CYBERSECUIRTY EFFORTS TO THE CYBERSECURITY FRAMEWORK.

The Cybersecurity Framework is a helpful tool for enterprise risk management, as are NIST's other frameworks that address IoT security,[24] secure software development,[25] as well as NIST guidance related to identity and access management for a variety of technologies, including healthcare.[26] The separation of these issues has created some confusion about where and when the Cybersecurity Framework and other guidance are applicable. NCTA therefore encourages NIST to consider linking its over-arching Cybersecurity Framework with these applied cybersecurity programs in a way that increases the cohesion of NIST's cybersecurity efforts and promotes more the adaptability and flexibility, which have been critical to the Framework's success thus far. This would aid in adoption of the Framework and attendant cybersecurity practices.

In particular, NIST can improve the usefulness of the Framework by further developing and promoting its National Online Informative References Program ("OLIR Program") to

[24] NISTIR 8259 Foundational Cybersecurity Activities for IoT Device Manufacturers, NIST (May 2020), https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/nistir-8259-series. Additionally, NIST published draft baseline security criteria for consumer IoT devices. *See* DRAFT Baseline Security Criteria for Consumer IoT Devices, NIST (Aug. 31, 2021), https://www.nist.gov/system/files/documents/2021/08/31/IoT%20White%20Paper%20-%20Final%202021-08-31.pdf.

[25] Secure Software Development Framework, NIST, https://csrc.nist.gov/Projects/ssdf (last accessed Apr. 25, 2022).

[26] NIST SP 1800-24, Securing Picture Archiving and Communication System (PACS): Cybersecurity for the Healthcare Sector, NIST (Dec. 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-24.pdf; *see also* NIST FIPS 201-3 Personal Identity Verification of Federal Employees and Contractors, NIST (Jan. 2022), https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-3.pdf. NIST has also published a Privacy Framework that is designed to assist organizations improve their privacy practices through enterprise risk management. NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0, NIST (Jan. 16, 2020), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf.

increase access to informative reference documents listed in the Cybersecurity Framework.[27] The OLIR Program is a NIST initiative that collects informative reference documents that are listed in the Cybersecurity Framework in order "to accommodate a greater number of Informative References and provides a more agile support model to account for the varying update cycles of all Reference Documents."[28] This program allows NIST and other organizations to develop and share best practices related to cybersecurity, which NIST compiles and shares on its publicly available website.

NIST can improve the OLIR Program by increasing the number of informative reference documents included in the database as additional informative references are added to the Cybersecurity Framework. Additionally, NIST can include a description of the OLIR program in the Cybersecurity Framework to notify users of the Cybersecurity Framework of how to access additional informative reference documents.

As an established process to develop and share best practices and standards that align with the Cybersecurity Framework, this program can influence and enhance the informative references to the Framework. NIST should allocate additional resources to the OLIR program to increase industry engagement in developing best practices and standards.

NIST should avoid revising the Cybersecurity Framework to attempt to address the specifics for all cybersecurity risks and instead aim to keep the Framework as a general, adaptable resource that can be used by varied organizations. Otherwise, such revisions would significantly limit the effectiveness and longevity of the Framework. Moreover, the Framework

[27] National Online Informative References Program, NIST, https://csrc.nist.gov/projects/olir/informative-reference-catalog (last accessed Apr. 25, 2022).

[28] NISTIR 8204 Cybersecurity Framework Online Informative References (OLIR) Submissions Specification for Completing the OLIR Template, NIST (Apr. 2019), https://www.govinfo.gov/content/pkg/GOVPUB-C13-c8ebe3bf0c53ac6e1f0023b2a11073cf/pdf/GOVPUB-C13-c8ebe3bf0c53ac6e1f0023b2a11073cf.pdf.

should reference many of the other frameworks and guidance that already closely align with the Framework. And, NIST should clarify in the Cybersecurity Framework how organizations can utilize and incorporate the guidance issued by NIST.

However, two areas that NIST should consider how to align more fully into the Framework are IoT and secure software development. These are important aspects of cybersecurity development. NIST should also encourage industry leaders to develop best practices regarding IoT security and secure software development and make such best practices available through the OLIR program.

V. NIST CAN BUILD ON THE SUCCESS OF THE CYBERSECURITY FRAMEWORK TO EFFECTIVELY ADDRESS SUPPLY CHAIN CYBERSECURITY ISSUES.

The Cybersecurity Framework was originally designed for organizational-level risk management, and its 2018 revisions in Version 1.1 now also incorporate supply chain risk management.[29] NIST should not make broad and sweeping revisions to the Cybersecurity Framework to address supply chain cybersecurity. Instead, NIST can promote adoption of the Framework and bolster its effectiveness by clarifying that it can be used by all Internet stakeholders, including supply chain manufacturers, which play a critical role in ecosystem-wide cybersecurity.

Collaboration among stakeholders is ongoing to build consensus concerning development of appropriate supply chain cybersecurity measures. As a result, any additional changes to the Cybersecurity Framework concerning supply chain security should be incremental to allow organizations to continue to gain knowledge about evolving threats and develop appropriate security solutions in response.

[29] Cybersecurity Framework, at 17.

Moreover, there has been significant action in federal agencies with respect to supply chain security. Rather than undertake significant revisions to the Framework, NIST should consider how targeted references to existing guidance from other federal agencies can be incorporated to promote a consistent and effective federal approach to supply chain cybersecurity. For example, within CISA, the Information and Communications Technology ("ICT") Supply Chain Risk Management Task Force ("SCRM Task Force") is "a public-private partnership charged with identifying challenges and developing actionable solutions to enhance global ICT supply chain resilience."[30] The SCRM Task Force has developed a standardized taxonomy of ICT supply chain elements, performed critical assessments of the ICT elements, and assessed national security risks stemming from ICT supply chain vulnerabilities.[31]

Likewise, NIST has provided guidance about technical aspects of supply chain issues, such as in response to President Biden's Executive Order 14028, pursuant to which NIST is working to develop standards concerning software supply chain security.[32] The Framework does not need to recreate or duplicate all these other efforts as many of them share or encourage companies and stakeholders to follow, key Framework guiding principles (secure authentication, identity and access management). Accordingly, NIST can refer to the work products of the SCRM Task Force and NIST's software supply chain guidance by creating a Framework Profile for SCRM as an appendix to the Framework.

[30] Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force, CISA, https://www.cisa.gov/ict-scrm-task-force (last accessed Apr. 25, 2022).

[31] *Id.*

[32] Software Supply Chain Security Guidance, NIST, https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/software-supply-chain-security-guidance (last accessed Apr. 25, 2022).

VI. CONCLUSION

The Cybersecurity Framework is a product of public and private collaboration and development over many years, and it has proven to be scalable and adaptable such that organizations of all sizes and complexities can adapt the Framework for their cybersecurity risks. These are the key strengths of the Framework, and NCTA encourages NIST to maintain that approach as it considers updating it.

We encourage NIST to focus on targeted revisions and clarifying additions that promote broad application and adoption of the Framework to help ensure that the Framework continues to be a useful and effective tool.

Respectfully Submitted,

/s/ Rick Chessen

Rick Chessen
Loretta Polk
Becky Tangren
NCTA – The Internet and Television Association
25 Massachusetts Ave., N.W. – Suite 100
Washington, DC 20001-1431
(202) 222-2445

Matthew J. Tooley
Vice President, Broadband Technology
Science & Technology

April 25, 2022