Before the Department of Commerce
Washington, D.C.

In the Matter of)
)
Views on the Framework for Improving) Docket No. 151103999-5999-01
Critical Infrastructure Cybersecurity)

COMMENTS OF CTIA – THE WIRELESS ASSOCIATION®

CTIA – The Wireless Association®
Expanding the Wireless Frontier
1400 16th Street, NW, Suite 600
Washington, DC 20036
(202) 736-0081
www.ctia.org

John M. Marinho
Vice President, Technology and Cybersecurity

February 23, 2016

TABLE OF CONTENTS

I. INTRODUCTION AND SUMMARY

CTIA – The Wireless Association® ("CTIA") is the international organization of the wireless communications industry, representing all parts of the global wireless ecosystem. CTIA appreciates the work of the National Institute of Standards and Technology ("NIST") to improve critical infrastructure cybersecurity, including developing the Framework for Improving Critical Infrastructure Cybersecurity ("Framework").[1] CTIA appreciates the opportunity to respond to this Notice and Request for Information ("RFI")[2] and offer suggestions for next steps.

The communications sector is fully engaged on cybersecurity. Through CTIA's Cybersecurity Working Group ("CSWG"), CTIA members representing the entire mobile ecosystem engage in research and dialogue with private sector and government entities including, in addition to NIST, the Department of Homeland Security ("DHS"), the Federal Communications Commission ("FCC"), and several others.[3] CTIA members are vigilant in protecting their networks and their customers' security and privacy. This hard work is paying off; America's wireless industry enjoys one of the lowest malware infection rates in the world.[4]

Since NIST released the Framework in 2014, the private sector has been integrating it into risk management strategies. Three lessons emerge: *First*, implementation is in its early stages, and the Framework is being used as designed. It is helping organizations manage risk, and is spurring the creation of derivative approaches. The Framework's fundamentals should remain unchanged so that adoption can continue. *Second*, it is vital that the Framework remain non-regulatory, voluntary, and focused on critical infrastructure. Government must resist efforts to regulate or use the Framework to set compliance expectations. *Third*, NIST should retain the lead role in federal efforts involving the Framework. Transition to private sector governance, at this time, is premature.

CTIA's comments track the structure of the RFI. Part II highlights attributes of the Framework's success. Part III addresses the communications sector's use of the Framework.[5] Part IV addresses updates.[6] Part V addresses member experiences sharing information about using the Framework.[7] Part VI addresses future governance.[8]

[1] NIST, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0* (Feb. 12, 2014) ("Framework"), *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf; *see also* 79 Fed. Reg. 9167 (Feb. 18, 2014) (announcing issuance of the Framework).

[2] *Views on the Framework for Improving Critical Infrastructure Cybersecurity*, Notice and Request for Information, 80 Fed. Reg. 76934, 76935 (Dec. 11, 2015) (NIST Docket No. 151103999-5999-01) ("RFI").

[3] *See* CTIA, *Today's Mobile Cybersecurity: Blueprint for the Future* 5 (2013), *available at* http://www.ctia.org/docs/default-source/default-document-library/cybersecurity_white_paper.pdf?sfvrsn=2.

[4] *See* CTIA, *Today's Mobile Cybersecurity: Information Sharing* 9 (2014), *available at* http://www.ctia.org/docs/default-source/default-document-library/ctia_informationsharing.pdf.

[5] *See* RFI, Question Nos. 1-9.

[6] *See id.*, Question Nos. 10-15.

[7] *See id.*, Question Nos. 16-19.

[8] *See id.*, Question Nos. 20-25.

CTIA appreciates NIST's leadership and urges NIST to continue promoting cybersecurity best practices in a collaborative, voluntary, and non-regulatory way.

II. THE NIST FRAMEWORK PROPERLY FOCUSES ON VOLUNTARY EFFORTS TO IMPROVE CRITICAL INFRASTRUCTURE CYBERSECURITY.

The challenges of evolving cyber threats will not be solved by regulation or checklists. They can only be met with innovation and agile, cross-sector cooperation. To promote collaboration and best practices, in February 2013 the President issued Executive Order 13636 and Presidential Policy Directive 21, directing Executive Branch entities to address critical infrastructure cybersecurity.[9] Section 7 of the Executive Order directs NIST to "lead the development of a framework to reduce cyber risks to critical infrastructure." The Framework must "incorporate voluntary consensus standards and industry best practices to the fullest extent possible" and "provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach."[10]

NIST responded. After convening government and private industry in various settings, NIST developed and released the Framework on February 12, 2014. "The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes."[11] It "uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses."[12]

Congress recognized NIST's success and codified its role in ensuring a non-regulatory approach.[13] As NIST has explained, the Cybersecurity Enhancement Act of 2014 "authorizes NIST to facilitate and support the development of voluntary, industry-led cybersecurity standards and best practices for critical infrastructure."[14] The Act flows from Congress's view that "NIST's partnership with industry to develop, maintain, and implement <u>voluntary</u> consensus standards related to cybersecurity best ensures the interoperability, security, and resiliency of the global infrastructure needed to make us all more secure."[15] The Cybersecurity Enhancement Act of 2014 also confirms a focus on "risks to critical infrastructure."[16] It adopts the definition of "critical infrastructure" in PPD-21, which covers "systems and assets, whether physical or

[9] Exec. Order No. 13636, Improving Critical Infrastructure Cybersecurity, 78 Fed. Reg. 11739 (Feb. 12, 2013) ("Executive Order"); Presidential Policy Directive/PPD-21, Directive on Critical Infrastructure Security and Resilience, 2013 Daily Comp. Pres. Doc. No. 00092 (Feb. 12, 2013) ("PPD-21").

[10] Executive Order § 7.

[11] Framework, at 1.

[12] *Id.*

[13] *See* Cybersecurity Enhancement Act of 2014, Pub. L. No. 113-274, 128 Stat. 2971 (2014) (codified in relevant part at 15 U.S.C. § 272).

[14] Confronting the Challenge of Cybersecurity, Hearing Before the Committee on Commerce, Science and Transportation, 114th Cong. 1 (Sept. 3, 2015) (testimony of Kevin Stine, Computer Security Division, Information Technology Laboratory, NIST) ("Stine Testimony").

[15] *Id*. at 5 (emphasis added).

[16] 15 U.S.C. § 272(c)(15).

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.[17] NIST and the rest of government are properly focused on critical infrastructure.

III. THE PRIVATE SECTOR IS USING THE FRAMEWORK TO POSITIVE EFFECT.

A. Government And Private Sector Entities Are Using The Framework.

The Framework is not a "checklist or a one-size-fits-all approach."[18] It was designed to be customized by critical infrastructure organizations, and it is helping both the government and the private sector. A recent survey of federal IT and security professionals found that 74 percent of the respondents' organizations use the framework as a "roadmap" for cybersecurity, while 68 percent said they use it to improve organizational security.[19] Thirty-nine percent of respondents said the standards helped to create a "uniform approach to discussing security" throughout their agency.[20] It has become a central part of federal cybersecurity policy and features prominently in legislative and executive action since its release.[21] States are using it as well. Shortly after its release, Virginia announced that the Framework would "help identify and communicate cybersecurity risks."[22] Pennsylvania's chief information security officer uses it to improve state enterprise governance.[23] Idaho and Mississippi "rely heavily" on the Framework for what the Brookings Institution characterized as a "truly outstanding" focus on cybersecurity.[24]

[17] *See id.* § 272(e)(3); 42 U.S.C. § 5195c(e).

[18] NIST, *Cybersecurity Framework Frequently Asked Questions: Framework Basics* (Oct. 21, 2015), http://www.nist.gov/cyberframework/cybersecurity-framework-faqs-framework-basics.cfm.

[19] Dell, *Dell Survey Reveals a Majority of Federal Agencies are Using NIST Cybersecurity Framework* (Dec. 8, 2015), http://www.dell.com/learn/us/en/vn/press-releases/2015-12-08-a-recent-dell-survey-fo-federal-it-professionals.

[20] *Id*.

[21] For example, the President recently established the Commission on Enhancing National Cybersecurity to "make detailed recommendations to strengthen cybersecurity in both the public and private sectors." Exec. Order No. 13718, Commission on Enhancing National Cybersecurity, 81 Fed. Reg. 7441, (Feb. 9, 2016). To accomplish this mission, the Commission is to "reference and, as appropriate, build on successful existing cybersecurity policies," *id.*, such as the Framework, *see* White House Office of the Press Secretary, Fact Sheet: Cybersecurity National Action Plan (Feb. 9, 2016), https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

[22] Press Release, Office of the Governor, *Governor McAuliffe Announces Virginia Adopts National Cybersecurity Framework* (Feb. 12, 2014), *available at* https://governor.virginia.gov/newsroom/newsarticle?articleId=3284#sthash.4o5XYhAU.dpuf.

[23] Brian Heaton, *Can We Talk: Creating a Common Language for Cybersecurity*, Government Technology (Oct. 7, 2014), *available at* http://www.govtech.com/security/Can-We-Talk-Creating-a-Common-Language-for-Cybersecurity.html.

[24] Gregory Dawson & Kevin C. Desouza, *How state governments are addressing cybersecurity*, Brookings Institution TechTank (Mar. 5, 2015), http://www.brookings.edu/blogs/techtank/posts/2015/03/5-state-cybersecurity-plans-dawson-desouza.

The private sector is using the Framework. For example, Intel reports: "the Framework has helped us harmonize our risk management technologies and language, improve our visibility into Intel's risk landscape, inform risk tolerance discussions across our company, and enhance our ability to set security priorities, develop budgets, and deploy security solutions."[25] There is evidence that the focus on risk management promotes adoption by "help[ing] organizations prioritize and validate investments" in cybersecurity.[26] Private sector use is not limited to critical infrastructure, the Framework's intended audience. In a recent survey of private IT professionals, three-quarters were able to identify significant cybersecurity risk "using the NIST Cybersecurity framework as a measuring stick."[27] Indeed, "the Framework is fast becoming the de facto standard for private sector cybersecurity."[28]

B. The Communications Sector Is Using The Framework In Multiple Efforts.

CTIA and the communications sector have worked with the Framework for some time.[29] It is an effective tool in the communications sector. For example, the Framework heavily influenced the work of the FCC's Communications Security, Reliability, and Interoperability Council ("CSRIC").[30] CSRIC IV Working Group 4 evaluated the Framework and mapped it across five industry segments: broadcast, cable, satellite, wireless, and wireline.[31] This effort involved over 100 experts from the communications sector, federal government, state government, equipment manufacturers, cybersecurity solution providers, and others. It resulted in the unanimous adoption of a detailed, 400-plus page Final Report that includes segment-

[25] Tim Casey et al., *The Cybersecurity Framework in Action: An Intel Use Case* 1 (2015), *available at* http://www.intel.com/content/www/us/en/government/cybersecurity-framework-in-action-use-case-brief.html.

[26] PricewaterhouseCoopers, *Why you should adopt the NIST Cybersecurity Framework* 4 (May 2014), *available at* https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/adopt-the-nist.pdf.

[27] *Survey: 75 percent of companies have significant risk exposure*, SC Magazine (June 11, 2015), http://www.scmagazine.com/more-than-400-security-pros-measured-their-security-programs-against-nist-framework/article/419974/.

[28] Richard Raysman & Francesca Morris, *CIOs Ignore the NIST Cybersecurity Framework at Their Own Peril*, Wall St. J. (Dec. 18, 2014), http://blogs.wsj.com/cio/2014/12/18/cios-ignore-the-nist-cybersecurity-framework-at-their-own-peril/.

[29] *See* RFI, Question Nos. 1-2.

[30] CSRIC is a federal advisory committee composed of leaders from the private sector, academia, engineering, consumer and non-profit organizations, and tribal, state, local, and federal agencies, and which provides the FCC with recommendations to ensure security and reliability of communications systems. *See Public Safety & Homeland Security Bureau Requests Comment on CSRIC IV Cybersecurity Risk Management & Assurance Recommendations*, Public Notice, 30 FCC Rcd 2363, 2363 n.1 (2015) ("CSRIC IV Public Notice").

[31] *See* CSRIC IV, Working Group 4, *Cybersecurity Risk Management and Best Practices: Final Report* 4 (2015) ("CSRIC IV Final Report"), *available at* https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

specific analysis of the Framework's application.[32] The FCC Chairman praised the Final Report as a major contribution to communications sector cybersecurity.[33]

The Framework is also relevant to efforts in CSRIC V. Working Group 5 is considering information sharing, including recommendations to the FCC for removing barriers to sharing among communications companies. Consistent with the Framework, efforts target the sector's ability to identify, protect, detect, respond, and recover from cyberattacks.[34] Working Group 6 is looking at secure hardware and software, and its ongoing work will use as a baseline or model approach the Final Report of CSRIC IV Working Group 4, which leveraged the Framework. Likewise, CSRIC V Working Group 7 is addressing cybersecurity workforce development. Efforts include demonstrating application of the National Initiative for Cybersecurity Education ("NICE") Cybersecurity Workforce Framework ("CWF") to work in the communications sector, including through an extended baseline of the NICE CWF Specialty Area Competencies and Knowledge, Skills, and Abilities metrics.[35] The NICE effort relies and builds on the Framework.

CSRIC is not the only way the communications sector is using the Framework. Industry groups, like CTIA's CSWG, are engaged. The CSWG promotes collaboration by technical and policy personnel from companies and government agencies. It produces white papers and comments. The Framework helps facilitate dialogue and align these efforts, and industry has been using it in numerous activities.

C. The Framework Core Is Proving Most Useful, And The Status Quo Should Be Preserved On Privacy.

The Framework Core has proven especially beneficial.[36] The Core is comprised of Functions, Categories, Subcategories, and Informative References, which together describe cybersecurity activities that are common across all critical infrastructure sectors.[37] The Core is helpful because it provides activities to achieve specific outcomes, and identifies available standards and guidance that can help achieve those outcomes.

CSRIC IV Working Group 4 Final Report demonstrated the Core's utility. Industry subgroups analyzed cybersecurity in the broadcast, cable, satellite, wireless, and wireline segments. The Wireless Segment Subgroup identified practices that align with the Framework

[32] *See* CSRIC IV Public Notice, 30 FCC Rcd at 2364.

[33] *See* David S. Turetsky, *Delving Into FCC's 'Damn Important' Cybersecurity Report*, Law360 (Mar. 30, 2015), http://www.law360.com/articles/636222/delving-into-fcc-s-damn-important-cybersecurity-report?article_related_content=1.

[34] *See* CSRIC V, Working Group 5, *Cybersecurity Information Sharing: Status Update* 2 (Sept. 21, 2015), *available at* https://transition.fcc.gov/bureaus/pshs/advisory/csric5/WG5_Presentation_092115.pptx.

[35] *See* CSRIC V, Working Group 7, *Cybersecurity Workforce: Status Update* 3, 7 (Dec. 3, 2015), *available at* https://transition.fcc.gov/bureaus/pshs/advisory/csric5/WG7_Presentation_120315.pptx.

[36] *See* RFI, Question Nos. 3-5.

[37] *See* Framework, at 18-36

Core and provided segment-specific practices companies can use to mitigate risk based on their risk profile, risk tolerance, and critical infrastructure ownership.[38]

The Wireless Segment Subgroup found that the Framework Core Functions, Categories, and Subcategories were particularly useful for articulating outcomes and illustrating use-case scenarios for wireless technologies, networks, and services. Using the National Sector Risk Assessment architecture model, the wireless section of the Final Report identified areas, assets, and services of critical focus.[39] It next provided guidance for aligning these elements with the Framework by tailoring the Functions, Categories, and Subcategories in a manner that best serves the wireless segment's cybersecurity challenges.[40] Finally, the wireless section of the Final Report provides an illustrative use case implementing the Framework.[41]

By contrast, the communications sector has found the Implementation Tiers less helpful, as they are not as practically applicable. If NIST were so inclined, it could clarify that the Tiers are not critical to using the Framework and that resources may be best focused on the Core.

Another notable part of the Framework involves privacy. The Framework's treatment of privacy was appropriately modest, and should not be adjusted now. NIST recognized that "[m]any organizations already have processes for addressing privacy and civil liberties," which the Framework should "complement" rather than try to replace.[42] Privacy and civil liberties issues are laden with policy judgments, which have to be balanced, as in legislation like the Cybersecurity Information Sharing Act of 2015 ("CISA").[43] To preserve the Framework's effectiveness and neutrality, NIST should retain the current approach to privacy.

D. The Framework Is Helping To Reduce Risk And Metrics Are Being Considered.

NIST asks whether the Framework has helped reduce cybersecurity risk, and whether metrics are available.[44] The Framework's efficacy is difficult to quantify; it is hard to measure both risk and the effects of preventive measures. "Security is difficult to measure and even harder to predict."[45] Industry observers note "a dearth of available options to effectively measure and assess cyber risk within a business context."[46] A notable consultancy states,

[38] *See* CSRIC IV Final Report, at 120-22.

[39] *Id.* at 128-31.

[40] *Id.* at 131-58.

[41] *Id.* at 159-64.

[42] Framework, at 3.

[43] Cybersecurity Information Sharing Act of 2015, Pub. L. No. 114-113, Division N §§ 101-11, 129 Stat. 2242 (2015) ("CISA").

[44] RFI, Question No. 8.

[45] CERT Div., Software Eng'g Inst., Carnegie Mellon Univ., *Cybersecurity Quality Metrics*, http://www.cert.org/cybersecurity-engineering/research/cybersecurity-quality-metrics.cfm? (last visited Feb. 23, 2016).

[46] Cory Mazzola, *The Business of Cyber Risk Assessment for Data Security*, IBM Security Intelligence (Apr. 15, 2015), https://securityintelligence.com/the-business-of-cyber-risk-assessment-for-data-security/.

"[C]ybersecurity risk is difficult to quantify. There's no single quantitative metric such as value at risk for cybersecurity, making it much harder to communicate the urgency to senior managers and engage them in required decisions."[47] Industry and government are working to measure risk and outcomes; in the meantime, the Framework is reducing risk by raising awareness, offering resources, and providing a common taxonomy for collaboration and information-sharing.

Work in CTIA's CSWG and the CSRIC confirm that the Framework complements existing practices and will contribute significantly to future efforts, such as information sharing.[48] The Framework is "providing the common language for industry groups, companies and government agencies to use in defining how information sharing can work to advance cybersecurity and protect privacy in a growing threat environment."[49] CTIA is not alone in this assessment. PricewaterhouseCoopers found that a common taxonomy "enable[s] security leaders to effectively communicate practices, goals, and compliance requirements with third-party partners, service providers, and regulators."[50] The Framework promotes dialogue about problems and opportunities, a key antecedent to collaboration that protects critical infrastructure.

E. NIST Should Continue To Champion A Voluntary, Non-Regulatory Approach.

NIST asks about Congressional direction to avoid multiplying duplicative regulatory processes.[51] This is a major concern. As Congress made clear, NIST should play a key role in protecting the Framework as a partnership. NIST has emphasized this, and should continue to champion the importance of government efforts remaining voluntary and non-regulatory.

Unfortunately, as federal agencies become more concerned about cyber threats, some appear to be inching toward regulation, compliance expectations, and reporting obligations—tacitly rejecting the voluntary model pioneered in the Framework and recognized by Congress in the Cybersecurity Enhancement Act of 2014. Agencies as varied as the FCC, the Securities and Exchange Commission ("SEC"), and the Federal Trade Commission ("FTC"), are signaling interest in oversight or enforcement when it comes to data and cybersecurity.

Likewise, some States are taking regulatory interest, increasing the risk of balkanization and redundancy. New York is considering "a new cyber security regulation for financial

[47] Tucker Bailey et al., McKinsey & Co., *Why senior leaders are the front line against cyberattacks* (June 2014), http://www.mckinsey.com/insights/business_technology/why_senior_leaders_are_the_front_line_against_cyberattacks.

[48] CTIA members participate in structured cybersecurity information sharing, for example, in the Communications Information Sharing and Analysis Center (Comm-ISAC), the National Cybersecurity and Communications Integration Center (NCCIC), DHS' Communications Sector Coordination Council (CSCC), the National Security Telecommunications Advisory Committee (NSTAC), among others.

[49] *See* CTIA, *supra* note 4, at 15.

[50] PricewaterhouseCoopers, *Why you should adopt the NIST Cybersecurity Framework* 4 (2014), *available at* https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/adopt-the-nist.pdf.

[51] *See* RFI, Question No. 9 (quoting 15 U.S.C. § 272(e)(1)(A)(vii)).

institutions" that would impose auditing and reporting obligations.[52] Connecticut is developing a "Cybersecurity Oversight Program" that asks private companies to participate in an effort that would enable government stakeholders to demand that companies develop and implement protective steps if government stakeholders perceive weakness in a company's cybersecurity. Communications companies have expressed serious reservations about this sort of effort, explaining that existing federal activities and processes should be the primary focus of scarce resources and collaborative effort.[53]

Burgeoning state and federal regulatory efforts would undermine the Framework. NIST has repeatedly emphasized that the Framework is "not a checklist," and that effective use requires a proactive, adaptable risk-management approach that prioritizes actions in light of evolving threats.[54] That is why NIST "convened meetings with regulators to discuss application of the Framework within the cyber ecosystem, and the need for the Framework to remain a voluntary methodology, adaptable to the critical infrastructure risk and mission objectives."[55] That also is why Congress has repeatedly disavowed a desire to confer cyber regulatory authority. [56] Prescriptive regulation, including compulsory reporting, undermines the NIST model by encouraging a check-the-box mentality at the expense of innovation and outcomes.

A regulatory approach can be counterproductive. For example, mandating disclosure of cybersecurity audit findings, as New York is considering, might discourage companies from undertaking audits, contrary to the gap analysis encouraged by the Framework.[57] And if audit results are disclosed—for example, pursuant to a Freedom of Information Act ("FOIA") request or as a result of a government data breach—it could cause competitive harm or provide a roadmap for malicious actors by revealing gaps.

Finally, a regulatory approach would chill collaboration that Congress and the President deem essential to cybersecurity. That is another reason why Congress has repeatedly disclaimed

[52] Memorandum from Anthony J. Albanese, Acting Superintendent of Financial Services to FBIIC Members re Potential New NYDFS Cyber Security Regulation Requirements 2 (Nov. 9, 2015), *available at* http://www.dfs.ny.gov/about/letters/pr151109_letter_cyber_security.pdf.

[53] *See PURA Cybersecurity Compliance Standards and Oversight Procedures*, Docket No. 14-05-12 (Conn. Pub. Util. Regulatory Auth. opened June 13, 2014). The Connecticut proposal may be based upon the misguided view that the NIST Framework "offers no solution" and that "state regulators and public utilities cannot use it as guidance." Conn. Pub. Util. Regulatory Auth., *Cybersecurity and Connecticut's Public Utilities* 8 (Apr. 14, 2014), *available at* http://www.ct.gov/pura/lib/pura/electric/cyber_report_041414.pdf.

[54] *See* Framework, at 7.

[55] Stine Testimony, at 8.

[56] *See, e.g.*, Cybersecurity Enhancement Act of 2014, Pub. L. No. 113-274, § 3, 128 Stat. 2971, 2972 (2014) ("Nothing in this Act shall be construed to confer any regulatory authority on any Federal, State, tribal, or local department or agency."); National Cybersecurity Protection Advancement Act, Pub. L. No. 114-113, Division N § 210, 129 Stat 2242 (2015) ("Nothing in this subtitle or the amendments made by this subtitle may be construed to grant the Secretary any authority to promulgate regulations or set standards relating to the cybersecurity of non-Federal entities, . . ."); CISA § 105(d)(5)(D) ("[C]yber threat indicators and defensive measures provided to the Federal Government under this title shall not be used by any Federal, State, tribal, or local government to regulate, including an enforcement action, the lawful activities of any non-Federal entity.").

[57] *See* Framework, at 14.

creation of regulatory authority, and why it placed responsibility for the Framework with NIST, a non-regulatory agency. The importance of cooperation free from the threat of regulatory consequence is evident in the information-sharing program created in CISA. Under CISA, because Congress included some agencies with regulatory authority in the program, it simultaneously instructed that information voluntarily shared "shall not be used by any Federal, State, tribal, or local government to regulate, including an enforcement action, the lawful activities of any non-Federal entity."[58] This prohibition reflects the risk of regulatory consequence stifling private-sector sharing with the government. The same concern applies in the context of the Framework, which is why Congress directed NIST to promote voluntary standards.[59]

NIST should continue to advocate the importance of maintaining a voluntary approach, and urge regulators at the state and federal level to resist the impulse to move toward new mandates, compliance oversight, or reporting requirements.

IV. NIST SHOULD LIMIT UPDATES TO THE FRAMEWORK AT THIS EARLY STAGE.

NIST should not make substantial revisions to the Framework now. Such revisions would be disruptive in this initial stage of implementation, as practices still are being mapped to it and it is being used to create additional guidance and training. Similarly, work identified in the Roadmap is ongoing, but these areas have not matured adequately for incorporation into the Framework. NIST should retain the existing, successful Framework.

A. Companies And Sectors Are Still Implementing The Framework.

Reports of ongoing implementation suggest it is premature to revise substantially the Framework. Many companies are in the early stages of applying it. A recent informal survey across 15 industry sectors found that 47 percent of "key executives and corporate counsel" did not know whether the NIST Framework had been helpful in managing their companies' cybersecurity risk.[60] Substantial revision at this time risks confusion, particularly for companies who are not yet sure how to use the Framework, and may cause additional delay in adoption.

Substantial revision at this early stage could create inefficiencies and setbacks, especially in the communications sector where, as discussed above, the industry has made significant strides in adapting the Framework to its needs. The CSRIC IV Working Group 4 Final Report contemplates that companies will need to assess sector-wide efforts in order to effectively apply them: "individual companies will have to go through these steps for themselves to develop their own cyber risk management programs, applying the framework to their own circumstances."[61] Industry groups and associations are incorporating the Framework into various efforts. If NIST

[58] CISA § 105(d)(5)(D)(i).

[59] *See* 15 U.S.C. § 272(e)(1)(A)(iii), (v) - (vii).

[60] Marcus Christian, *Corporate Perspectives On Cybersecurity: A Survey Of Execs*, Law360 (May 6, 2015), http://www.law360.com/articles/644868/corporate-perspectives-on-cybersecurity-a-survey-of-execs.

[61] CSRIC IV Final Report, at 120.

were to substantially revise the Framework, industry and individual companies' use may be impeded.

Substantial revision now could also negatively affect the work of CSRIC V. For example, if changes to the Framework were to require revisions to derivative work like the NICE CWF, Working Group 7's focus on aligning cybersecurity workforce development with the CWF would be undermined. Extensive changes to the Framework might also divert resources as CSRIC V realigns its other working groups to reconsider the Framework. So much has already been built on the Framework, it is crucial to keep it in place and unchanged.

B. Efforts In Areas Identified By The Roadmap Continue To Mature.

NIST asks whether developments in the nine areas identified in the Roadmap should inform changes to the Framework.[62] Progress is being made in these areas, but they have not matured, and ongoing development efforts counsel in favor of stability.

Several of the high-priority areas identified in the Roadmap are complex and in a state of flux. For example, the Roadmap identifies automated indicator sharing as a potential area for development, alignment, and collaboration.[63] Provisions in the recently enacted CISA are promising and will help foster creativity and increased collaboration. But these statutory provisions anticipate forthcoming guidance from DHS and the Department of Justice, which will establish policies and procedures for automated indicator sharing.[64] Attempts to capture this rapidly changing environment in the Framework risks violating NIST's statutory mandate to "prevent duplication of . . . related processes."[65] In the meantime, CTIA's CSWG plans an automated information sharing pilot program in 2016 based on the STIX, TAXII, and CybOX protocols.[66] Other sectors may be planning their own programs. NIST should foster such experimentation, but there is no one solution for everyone, and it may not be possible to capture in the Framework the diversity of experience at this preliminary stage.

Other complex areas are still under consideration. The Roadmap identifies authentication as an issue for continued attention, due in large part to the varied settings in which authentication is critical.[67] NIST is learning from the National Strategy for Trusted Identities in Cyberspace ("NSTIC") and the privately-led Identity Ecosystem Steering Group ("IDESG"), and integrating it into NIST Special Publication guidance. Such efforts remain ongoing because authentication is a broad concept subject to continuing innovation, evolving federal requirements, and an

[62] RFI, Question No. 14.

[63] *See* NIST, *Roadmap for Improving Critical Infrastructure Cybersecurity* § 4.2 (Feb. 12, 2014) ("Roadmap"), *available at* http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf.

[64] CISA § 105(a).

[65] 15 U.S.C. § 272(e)(1)(A)(vii).

[66] *See* DHS US-CERT, *Information Sharing Specifications for Cybersecurity*, https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity (last visited Feb. 23, 2016) ("TAXII, STIX and CybOX are community-driven technical specifications designed to enable automated information sharing for cybersecurity situational awareness, real-time network defense and sophisticated threat analysis.").

[67] *See* Roadmap § 4.1.

advanced threat landscape targeting remote authentication.[68] The Framework is not the right vehicle for incorporating the level of detail achievable through authentication-specific guidance. Best practices depend on context, so anything more in the Framework than a general recognition of the importance of authentication in varied settings would be too granular.

Similarly, supply chain management and cybersecurity are complex issues, currently being examined in various settings.[69] NIST is in the process of convening stakeholders and evaluating issues.[70] Industry is aware of how supply chain and vendor management impacts organizational, device, and service cybersecurity. Solutions are under consideration, but it would be premature to include supply chain cybersecurity in an updated Framework.

Likewise, NIST has been working on international standardization,[71] as directed by the Cybersecurity Enhancement Act of 2014 and called for in the Roadmap. International standardization is critical because "[d]iverse or specialized requirements can impede interoperability, result in duplication, harm cybersecurity, and hinder innovation."[72] NIST's efforts should continue, and incorporation into the Framework would be premature.

Privacy efforts at NIST are similarly nascent, and are not good candidates for inclusion in updates to the Framework. NIST recently observed that "few technical standards or best practices exist to mitigate the impact of cybersecurity activities on individual privacy and civil liberties."[73] NIST has recognized that technical privacy standards are "context-dependent and relatively subjective."[74] Many NIST efforts on privacy look to federal government settings and are not readily applicable to the private sector. Even if such efforts were presently adaptable to the Framework, adding privacy is not necessary at this time. The private sector is engaged on privacy. For example, the mobile industry has developed and adheres to guidelines, including the "Consumer Code for Wireless Service," a voluntary commitment to provide understandable policies, and efforts by associations like the Mobile Marketing Association's Mobile Privacy Guidelines. Industry policies emphasize the importance of educating consumers and facilitating their control of information. Extending the Framework into these areas is unlikely to help

[68] *See, e.g.*, NIST, *NIST Solicits Comments on its Electronic Authentication Guideline* (Dec. 15, 2015), http://csrc.nist.gov/groups/ST/eauthentication/sp800-63-2_call-comments.html (updating Special Publication 800-63-2 in response to developments and the Framework's call to ". . .conduct identity and authentication research complemented by the production of NIST Special Publications that support improved authentication practices.").

[69] *See* Roadmap § 4.8.

[70] *See* NIST, *Supply Chain Risk Management (SCRM) for Information and Communications Technology* (July 29, 2015), http://csrc.nist.gov/scrm/. NIST held a workshop on supply chain cybersecurity best practices in October 2015 and is actively engaging the issue. *See* NIST, *Best Practices in Cyber Supply Chain Risk Management* (Jan. 14, 2016), http://www.nist.gov/itl/csd/best-practices-in-cyber-supply-chain-risk-management-october-1-2-2015.cfm. As CTIA has pointed out, the complexities of global supply chains involving hardware, software, applications, and cloud offerings make generalizing best practices a challenge.

[71] *See* NIST, *Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity*, NISTIR 8074 (Dec. 2015) ("NIST Interagency Report").

[72] Roadmap § 4.7.

[73] *See* NIST Interagency Report, at 11.

[74] Roadmap § 4.9.

protect consumers, and applicable approaches may be too complex or context-specific to be imported meaningfully into the Framework.

C. Minor Course Corrections May Be Appropriate.

NIST might consider minor modifications that would not upset ongoing implementation. As NIST suggests, one way to do this might be to remove elements of the Framework that have proven less effective.[75] As noted, CTIA members have found that the Framework Implementation Tiers are not particularly useful. If this experience is shared in other sectors, NIST might consider deleting the Framework Implementation Tiers.

NIST should resist adding new elements. Brevity helps to discourage a compliance checklist mentality, and a concise document is better suited to adaptation across a diverse set of industry sectors and segments, where details will by necessity need to be worked out. The Framework has been pushed out broadly and entities are still figuring out how to use it. Innovation depends on Framework stability, so it makes sense to leave it alone for now.

V. THE PRIVATE SECTOR SHARES INFORMATION ABOUT THE FRAMEWORK IN A VOLUNTARY AND COLLABORATIVE MANNER.

NIST asks for information about information sharing among private sector entities on using the Framework.[76] The communications sector has been active in developing best practices and sharing information about use of the Framework and other risk-management resources.[77]

A. The Communications Sector Is Sharing Information About The Framework Through CTIA And Other Industry Forums.

The communications sector actively shares information across many forums. CSRIC is one example of a good model in the industry. As noted above, CSRIC IV mapped the NIST Framework across five communications industry segments. This activity provided a vehicle for members of the broadcast, cable, satellite, wireless, and wireline segments to share information and experiences regarding the Framework with each other.[78]

Information sharing about the Framework has also been pursued by developing use cases, often through trade associations. Such uses cases relate to critical infrastructure and ancillary systems that may be relevant, in particular when combined with efforts like the Information Sharing Pilot to be led by CTIA. Such voluntary, third-party efforts increase the willingness and ability to share information.[79] Recent legislation clarifying that it is not an antitrust violation to

[75] RFI, Question No. 11.

[76] *Id.*, Question Nos. 16-19.

[77] Cybersecurity information sharing is a broad topic with policy implications. *See* CTIA, *supra* note 4. NIST here is focused on sharing information about the use of the Framework.

[78] *See* CSRIC IV Final Report, at 4.

[79] *See* RFI, Question No. 19.

share certain information for cybersecurity purposes may help promote collaboration and sharing, which may extend to sharing concerning the Framework.[80]

A variety of information-sharing and analysis centers ("ISACs") and information sharing and analysis organizations ("ISAOs") enable companies to share best practices and threat information, including by the communications sector. Among other venues, the DHS NCCIC, and its National Coordinating Center for Communications ("NCC") enable communication industry collaboration.[81] There, dozens of federal agencies and over fifty private sector communications and IT companies share critical communications information and advice. Congress and the Executive Branch want to expand the utility of the NCCIC and ISACs, and to develop additional ISAOs. For example, DHS has been promoting voluntary standards for ISAOs under Executive Order 13691, Promoting Private Sector Cybersecurity Information Sharing.[82] These entities are designed to be inclusive of all private sector entities who want to be involved and provide additional opportunities for sharing information.

B. The Government Should Not Chill Information Sharing Through The Specter Of Regulation.

Despite positive developments, an emerging dynamic may chill collaboration with the government.[83] Some regulators have expressed interest in receiving "assurances" about private sector use of the Framework and concomitant cybersecurity improvements.[84]

Regulated parties may be concerned about how information shared with regulatory agencies outside a construct like CISA could be used. For example, if a private entity were to share a gap analysis, a regulator might use information to press for more data, suggest operational changes, justify regulation, or initiate an enforcement action. CISA validates such concerns. Congress recognized that fear could chill desired information-sharing and cripple the program. So it expressly prohibited regulatory bodies from taking regulatory or enforcement

[80] *See* CISA §§ 104(e), 108(e).

[81] *See supra* note 48 (identifying NCCIC and other entities).

[82] 80 Fed. Reg. 9349 (Feb. 13, 2015); *see also* DHS, *Information Sharing and Analysis Organizations* (Dec. 14, 2015), http://www.dhs.gov/isao.

[83] *See* RFI, Question Nos. 17-18.

[84] *See, e.g.*, *Remarks of FCC Chairman Tom Wheeler As Prepared for Delivery at the RSA Conference, San Francisco, Ca.*, 2015 WL 1849652, at *2 (FCC Apr. 21, 2015) ("CSRIC developed a range of activities intended to provide transparent assurances to the FCC, to DHS, to industry, and to consumers. These visible assurances should provide confidence that companies throughout the sector are actually taking effective steps to manage cyber risk."); *Remarks of SEC Commissioner Luis A. Aguilar as Prepared for Delivery at the NYSE "Cyber Risks and the Boardroom" Conference, New York, N.Y.* (June 10, 2014) ("While the Framework is voluntary guidance for any company, some commentators have already suggested that it will likely become a baseline for best practices by companies, including in assessing legal or regulatory exposure to these issues or for insurance purposes. . . . [B]oards should work with management to assess their corporate policies to ensure how they match-up to the Framework's guidelines — and whether more may be needed."), *available at* http://www.sec.gov/News/Speech/Detail/Speech/1370542057946.

action in response to information shared under CISA.[85] Outside such a regime, where information is needed by an agency, it would be preferable to provide information to non-regulatory bodies or to third parties that would aggregate and anonymize relevant data.

Another concern is the burden imposed by proliferating requests at the federal, state, and local level, and attendant risks of disclosure. A great deal of information already is shared with DHS and other agencies, including through ISACs. Multiple requests can result in needless duplication and even seemingly modest requests impose burdens. Organizations must gather information and mitigate risks from disclosures under regimes like the FOIA and equivalent state laws. Those risks are real; information in the wrong hands can be competitively harmful or identify opportunities to exploit. Companies are careful about what they provide the public and regulators. The protections included in CISA validate these concerns too: under CISA, Congress exempted from FOIA disclosure information voluntarily shared in that program.[86] Similar accommodations may promote sharing in other contexts; NIST should consider how to mitigate such concerns beyond CISA.

VI. NIST SHOULD RETAIN FRAMEWORK GOVERNANCE FOR THE FORESEEABLE FUTURE.

NIST requested input on the future governance of the Framework, including a transition to the private sector.[87] NIST should maintain a leading role for the foreseeable future. A public-private partnership with diverse stakeholders is key to maintaining the Framework's momentum.

If NIST were to consider a transition to the private sector, it would have to answer difficult questions. For example, it might be difficult to maintain a sufficiently broad perspective across sectors. There are over a dozen identified critical infrastructure sectors, and other industries are making use of the Framework. Different sectors may have different goals in the development or application of the Framework, so it would be important to identify a neutral governing entity that would not be disposed to capture by a particular industry. Establishing an operating structure is another challenge. Some groups operate by consensus; others vote. Another question is timing, particularly related to international harmonization and whether a governing entity should be U.S.-focused or include global stakeholders.

A transition would also require an entity to provide or generate substantial resources, financial and otherwise. For example, an entity would need the requisite technical skill to ensure that the Framework remains a useful paradigm. And it would need to be well positioned to draw on government and private sector expertise in order to maintain credibility with both spheres.

[85] *See* CISA § 105(d)(5)(D)(i) ("[C]yber threat indicators and defensive measures provided to the Federal Government under this title shall not be used by any Federal, State, tribal, or local government to regulate, including an enforcement action, the lawful activities of any non-Federal entity.").

[86] *See id.* § 105(d)(3) ("A cyber threat indicator or defensive measure shared with the Federal Government under this title shall be—(A) deemed voluntarily shared information and exempt from disclosure under section 552 of title 5, . . . and (B) withheld, without discretion, from the public under section 552(b)(3)(B). . . .").

[87] *See* RFI, Question Nos. 20-25.

There are models for transitioning standards and activities to private or international bodies. But at this time, a change in governance is premature. More time is needed to ensure the efficacy of the current model, and to promote meaningful participation by all stakeholders.

VII. CONCLUSION

The NIST Framework continues to improve critical infrastructure cybersecurity. It works because it is non-regulatory, voluntary, and collaborative. Government should recognize these reasons for its success, and resist any impulse to turn to regulation or convert the Framework into a reporting or compliance obligation. NIST has become a leading voice in the national cybersecurity dialogue and has provided the country with vital foundational principles to address cyber risks. NIST should continue to shape this important national discussion.

Respectfully Submitted,

CTIA – The Wireless Association®
Expanding the Wireless Frontier
1400 16th Street, NW, Suite 600
Washington, DC 20036
(202) 736-0081
www.ctia.org

John M. Marinho
Vice President, Technology and Cybersecurity

February 23, 2016