Before the Department of Commerce
National Institute of Standards and Technology
Washington, D.C.

In the Matter of	**)**	
	)	
Developing a Framework to Improve	**)**	**Docket No. 130909789–3789–01**
Critical Infrastructure Cybersecurity	**)**	

Comments of CTIA- The Wireless Association®, the National Cable & Telecommunications Association and the US Telecom Association

on the

Preliminary Cybersecurity Framework Released by the National Institute of Standards and Technology

CTIA- The Wireless Association
Michael Altschul, Senior Vice President, General Counsel
John Marinho, Vice President, Cybersecurity
Debbie Matties, Vice President – Privacy

National Cable & Telecommunications Association
Rick Chessen, Senior Vice President, Law and Regulatory Policy
Loretta Polk, Vice President and Associate General Counsel
Matt Tooley, Senior Director, Broadband Technology

US Telecom Association
Jon Banks, Senior Vice President, Law and Policy
Robert Mayer, Vice-President, Industry and State Affairs

TABLE OF CONTENTS

CTIA-The Wireless Association®, the National Cable & Telecommunications Association ("NCTA") and the US Telecom Association ("USTA") (collectively, the "Associations") respectfully submit these comments on the Preliminary Framework released by the National Institute of Standards and Technology ("NIST").

I. INTRODUCTION

CTIA, NCTA, and USTA have been active participants in the policy and technical discussions about cybersecurity and the NIST Preliminary Framework, and submit these comments to share the perspective of the communications industry. This industry illustrates the diversity of potential use cases for the Framework; sectors include wireless, wireline, and cable, which deliver voice, data, internet access, and more. Our members range from small businesses to multinational corporations who develop and provide innovative services, products, and technology to serve customers of all sizes around the world.

CTIA's membership spans the mobile wireless ecosystem, from device manufacturers and wireless carriers to software and application developers, among others. These companies have led a global, mobile revolution. This growth has transformed the economy and benefited consumers, but it also provides opportunity for cybercriminals. To address these threats, CTIA created a Cybersecurity Working Group ("CSWG"), comprised of senior technical and policy representatives from leading companies. CTIA's CSWG facilitates innovation and cooperation on advanced responses to evolving threats, as well as the formulation of policy positions and white papers in collaboration with government officials. CTIA has actively participated in the federal government's cybersecurity activities, including efforts of NIST.[1]

NCTA represents the cable industry, which delivers broadband, video, and voice via two-way interactive networks with fiber optic technology. As leaders in the digital revolution and the nation's largest providers of broadband service, NCTA's member companies have been at the forefront of developing and implementing a broad range of practices and protocols for identifying and addressing cybersecurity risks and vulnerabilities. To assist with member company coordination on cybersecurity, NCTA established a Cybersecurity Working Group, comprised of senior technical and policy representatives from cable companies, to identify tools and technology for detecting threat information and share best practices in all areas related to cybersecurity.

USTelecom represents broadband service providers and suppliers for the telecom industry. USTelecom's diverse member base ranges from large publicly-traded communications corporations to small private cooperatives—all providing advanced communications services to markets both urban and rural. As the Internet becomes more widely available across the globe, cyber-attacks become an increasing presence as well, and USTelecom's members play an important role in this diverse and interconnected ecosystem. USTelecom's Cybersecurity Working Group includes legal, technical, and policy representatives from our member

[1] Simultaneously with this filing, the Associations submit accompanying comments in the template form provided by NIST ("CTIA/NCTA/USTA Template Submission").

companies that work collaboratively to identify and develop tools and practices for enhancing cybersecurity.

A variety of communications sector public-private partnerships and efforts are underway that address cybersecurity, including the Communications Sector Coordinating Council (CSCC), which actively coordinates government and private actors to ensure the nation's communications systems are secure and resilient. Other examples include the National Communications System ("NCS") and the United States Computer Emergency Readiness Team ("US-CERT"). Communications companies engage in ongoing research and dialogue with other agencies like NTIA, Defense Information Systems Agency, and the Department of Homeland Security, in addition to a variety of working groups. Robust public-private partnerships assist the federal government with flexible solutions to national security and emergency preparedness.

Within and outside these partnerships, the communications industry, whether it be wireless, wireline, or cable, responds to the full array of cyber threats that evolve at breakneck speed and require agile responses. Our companies' business success depends on customers using our services in a safe and secure environment. As a top business priority, our companies devote substantial capital, resources, and personnel to prevent, detect, deter, and respond to cybersecurity threats, without any express government directive to do so. Securing our networks against cyber threats is a business imperative for the communications industry. This is a matter of not only acquiring and deploying technological tools, but an organizational and managerial undertaking at all levels of the companies. Communications networks differ, so participants in each sector address security in diverse ways, consistent with the relevant network architecture, threat profile, and user expectations. Based on our members' experiences, CTIA, NCTA, and USTA believe that, to be successful, any cybersecurity Framework should provide clarity and flexibility for those enterprises that will evaluate whether and how to use it. To that end, our comments first focus on the development of a voluntary framework based on collaboration with multiple industry and government stakeholders. Such an approach spurs the innovation and experimentation necessary to avoid a static and regimented regime that produces an ineffective "check-the-box" compliance mindset. Our comments then focus on narrowing the breadth of the sweeping privacy and civil liberties provisions in the proposed privacy methodology.

II. SUMMARY OF COMMENTS

President Obama issued Executive Order 13636 and Presidential Policy Directive, PPD-21, in February 2013, directing Executive Branch entities to take action on cybersecurity.[2] Among the many actions outlined in those documents, 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."[3] This Framework is intended to be part of the Voluntary Program

[2] Executive Order 13636 – Improving Critical Infrastructure Cybersecurity, rel. Feb. 12, 2013 ("Executive Order"); Presidential Policy Directive/PPD-21, Critical Infrastructure Security and Resilience, rel. Feb. 12, 2013 ("PPD-21").

[3] Executive Order, at § 7.

to be developed by the Department of Homeland Security ("DHS"),[4] and it will also be used by sector-specific agencies evaluating the adequacy of their authorities and regulations.[5]

On October 22, 2013, after holding several public workshops and synthesizing a vast amount of information in a short time period, NIST released the Preliminary Framework.[6] The draft seeks to help organizations to "identify and prioritize actions for reducing cybersecurity risk" and foster cybersecurity improvement by utilizing industry-known standards and best practices.[7] The Preliminary Framework is made up of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profile, and it includes a user's guide and a section for senior executives on using the Framework to evaluate preparedness for cybersecurity events.

CTIA, NCTA, and USTA applaud NIST's efforts in developing the Preliminary Framework in a transparent, inclusive, industry-driven, consensus-based manner that has been responsive to industry throughout the workshop process. NIST's approach serves the government's ultimate goal of having industry embrace the Framework. In particular, the Associations appreciate the efforts reflected in the recently released clarification document, which explains how organizations can "adopt" and "use" the Framework.[8]

Evaluation of the Preliminary Framework disconnected from the future Voluntary Program of which it will be a part is quite a challenge, especially amid uncertainty about agencies' regulatory goals and legislative activity. Notwithstanding these challenges, to assist NIST's efforts to improve the Framework that will emerge from these documents, CTIA, NCTA, and USTA respectfully propose the following changes to clarify and simplify the Framework's operation and use.

First, as explained in Part III, the Associations propose changes to ensure that the Preliminary Framework is truly voluntary, and to clarify how organizations may use the Framework. While the recent clarification document is a positive step that may well encourage industry use, additional clarifications will help "provide sufficient guidance to aid businesses of all sizes while maintaining flexibility."[9] In a future DHS program or otherwise, the voluntary nature of Framework use will be important to ensure that its efforts can scale effectively from large to small organizations. DHS therefore should not mandate adherence to particular aspects, and NIST should clarify that those who do use the Framework may choose alternative methods. In addition, NIST should explain that an organization can "use" the Framework by leveraging any existing cybersecurity program, including when the program has been certified as compliant with existing, independent standards and best practices. To the degree that organizations refer to

---

4 *Id.* at § 8.

5 *Id.* at § 10.

6 National Institute of Standards and Technology, *Improving Critical Infrastructure Cybersecurity, Executive Order 13636, Preliminary Cybersecurity Framework* (Oct. 22, 2013), *available at* http://nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf ("Preliminary Framework").

7 *Id.* at 5.

8 NIST, *Update on the Development of the Cybersecurity Framework* 1 (Dec. 4, 2013).

9 *Id.*

the Framework and use it to evaluate and improve their cybersecurity, the Framework will have achieved its goal.

Second, as explained in Part IV, CTIA, NCTA, and USTA are concerned about the breadth of the privacy and civil liberties provisions, in Appendix B. Those provisions are too broad, complex, and open-ended; they are inadequately tailored to privacy risks related to cybersecurity activities; they inappropriately incorporate privacy standards developed for government agencies; and they do not reflect industry consensus. The Executive Order instructs NIST to develop a framework "to reduce cyber risks to critical infrastructure," not a broad framework to address or improve private sector privacy policies. The Framework's proposed privacy methodology could chill use of the Framework. NIST should limit the privacy methodology to the privacy risks associated with protective cybersecurity activities, eliminate redundancy with regard to information protection functions in Appendix A, and avoid sweeping guidance or recommendations related to civil liberties which are primarily a concern of state actors. NIST should consider replacing Appendix B with an alternative consensus methodology that addresses the collection and use of "protected information" related to an organization's cybersecurity activities.

There is still work to be done by the private sector and the government, in processes outside of NIST's control, including at DHS regarding the Voluntary Program and incentives. CTIA, NCTA, and USTA offer thematic suggestions in this draft, including particular edits in the requested Template, attached hereto, and the Associations support inclusion of the Alternative Privacy Methodology that has already been submitted on behalf of an industry-wide working group. CTIA, NCTA, and USTA remain willing to assist NIST in improving the Framework to advance the nation's cybersecurity.

III. THE FRAMEWORK NEEDS ADDITIONAL CLARIFICATIONS TO ENSURE IT IS TRULY VOLUNTARY, FLEXIBLE, AND SCALABLE.

NIST asks whether the Framework is "presented at the right level of specificity."[10] The Framework may be used by a Critical Infrastructure ("CI") owner participating in a future Voluntary Program, or it may be consulted by a non-CI owner interested in improving its cybersecurity profile. Thus, while the Framework can help organizations evaluate their cybersecurity posture and identify helpful options, CTIA, NCTA, and USTA propose that it include explicit language confirming that its use is intended to be voluntary and flexible, and avoid words and constructions that might have unintended consequences.

A. NIST Should Include Specific Language to Clarify That Use of the Framework Is Purely Voluntary.

The Executive Order is premised sensibly on the notion that industry has the right to choose whether to use the Cybersecurity Framework. The Executive Order states that "[t]he Cybersecurity Framework shall incorporate *voluntary* consensus standards and industry best practices" and "shall be consistent with *voluntary* international standards."[11] NIST notes that a

[10] *Id.*

[11] Executive Order, § 7(a). (Emphasis added.)

goal of the Framework is to "be an adaptable, flexible, and scalable tool for *voluntary* use."[12] In the Section entitled "*Voluntary* Critical Infrastructure Cybersecurity Program," the Executive Order mandates that DHS "establish a *voluntary* program to support the use of the Cybersecurity Framework by owners and operators of critical infrastructure and any other interested entities."[13] While the government might encourage industry to use the Framework, organizations must maintain the ability to choose whether to use it without penalty.

The communications industry shares NIST's and the Administration's goal of thwarting cyber attacks. To empower organizations across industries to help with this goal, the private sector must be encouraged to evaluate its own networks and systems and use its own judgment to determine the best approach to protect critical infrastructure. To encourage use of and reference to the Framework, NIST must make clear that the Framework is truly voluntary and its use by a company will not have any binding legal or regulatory effect.

The Framework should make clear that it is not intended to have any binding legal or regulatory effect. Voluntary standards and best practices form the basis of the Framework, and a "significant difference between regulations and standards involves the coercive power of regulations."[14] With voluntary standards, "individuals and firms can, if they choose, elect not to adhere to the standard;" however, "unlike private standards, many regulations are not 'voluntary.'"[15] NIST should make clear that the Framework is not intended to create obligations, rights, or responsibilities by including the following language: "Use of the Framework is purely voluntary. The Framework is not intended to create any rights or obligations or be used as basis for liability or responsibility in any legal or regulatory proceeding." This language should be placed in the Introduction section and Appendix A.

In many places NIST explains that the Framework "can" be used in certain ways, implying that organizations are free to choose to use it and select options from it.[16] This is helpful, but it should be strengthened. CTIA, NCTA, and USTA propose additional language throughout the document to confirm that its provisions only apply to those organizations that voluntarily choose to use it. For example:

- When referencing "organizations," NIST should include modifiers that make clear that the organizations discussed are "organization(s) voluntarily seeking to use or implement the Framework."
- In several places, NIST should replace the words "should" and "can" with "may" to avoid confusion about the required nature of the guidance. In other places, NIST should add language to clarify that its word choices, including present-tense

---

12 Preliminary Framework, Appendix D, at 40 (emphasis added).

13 Executive Order, § 8(a) (emphasis added).

14 David J. Teece & Edward F. Sherry, *Standards Setting and Antitrust*, 87 Minn. L. Rev. 1913, 1919 (2003).

15 *Id.*

16 *See e.g.*, Preliminary Framework, at § 2.0 ("The Framework can be used to help identify…and is a tool…" that entities "can use . . . for different means…") (emphasis added); *id.* § 2.1 ("The Framework Core is not a checklist of activities to perform…"); § 2.2 ("A Framework Profile can be used . . ..") (emphasis added). Such language, after replacing the word "can" with "may," should be added to other sections of the Framework.

constructions, are not construed as commands or normative descriptions. *See also* CTIA/NCTA/USTA Template Submission, at No. 62.

To provide more clarity for readers of the document, NIST should define "may" and similar directives, such as "can," where those words are used (the definition should be the same). Standards documents often include definitions of such words, but they are not included in NIST's Glossary. NIST could model its definition of "may" on definitions in IETF RFC 2119[17] and add them to the Glossary. Specifically, after making many of the replacements identified herein, NIST should define the word "may" as: "This and similar words mean that an item is truly optional. An organization electing to use the Framework may choose to use a certain aspect of the Framework, while another organization may omit the same item."[18] *See also* CTIA/NCTA/USTA Template Submission, at No. 88.

Without explicit limiting language, the Framework could be used in ways that could transform voluntary guides into *de facto* requirements. This could happen if the Framework is used in legal proceedings to inform or impose liability for actions or failures to act, or by regulators evaluating regulation or taking enforcement action. Such use of the Framework could be "disruptive to effective cybersecurity practices in use today."[19]

Another barrier to eventual use of the Framework is the prospect of third-party auditing or disclosures. This is why the Associations oppose government-sponsored or required auditing, certification or reporting process to assess, document or evaluate organizations' use of the Framework. Requiring audits or reviews, as suggested by the PCAST's recent *Report to the President: Immediate Opportunities for Strengthening the Nation's Cybersecurity*,[20] is not a desirable approach. Any government-imposed audit requirement would be inconsistent with a voluntary Framework that is flexibly used and implemented by diverse organizations. While many enterprises choose to rely on security audit activities, a Framework-related audit process would be a disincentive to use of the Framework by creating a counter-productive, redundant, or burdensome regime. Moreover, it creates risk, particularly if information about organizations' internal evaluations or use of the Framework is disclosed. Care should be taken to emphasize that the Framework's tools are for voluntary, internal use and not designed as a basis for public or regulatory disclosures. This applies to all uses of the Framework, including any determinations about the Framework Profile in Section 2.2, or the Implementation Tiers in Section 2.4.[21] Required disclosures could lead effectively to mandatory use that would

---

[17] The Internet Engineering Task Force (IETF), IETF RFC 2119: *Key words for use in RFCs to Indicate Requirement Levels* (Mar. 1997), *available at* http://www.ietf.org/rfc/rfc2119.txt.

[18] If NIST retains the word "should" in the Framework, but intends that it not be interpreted as a command or recommendation, NIST should define word "should" per the definition of "may" given in these comments.

[19] Preliminary Framework, at i.

[20] Executive Office of the President, President's Council of Advisors on Science and Technology, *Report to the President, Immediate Opportunities for Strengthening the Nation's Cybersecurity* 2 (Nov. 2013).

[21] NIST recognizes that Profiles can aid internal use, *see* Preliminary Framework at 3 ("Profiles can be used to conduct self-assessments and communicate within an organization or between organizations."), but the language should be strengthened to ensure that such information is for internal use, and external sharing is only in the organization's discretion.

undermine the voluntary nature of the Framework and reduce the incentive to use it.[22] NIST should consider clarifying that the processes contemplated in the Framework for deciding whether and how to use it are not susceptible to third-party auditing, certification, or disclosures.

B. The Framework Should Explicitly Promote Flexibility in Use.

Entities in the communications industry already develop solutions based on industry-wide best practices, collaborative efforts, codes of conduct, as well as their organizations' needs and capabilities. The PPD-21 states that "[c]ritical infrastructure owners and operators are uniquely positioned to manage risks to their individual operations and assets, and to determine effective strategies to make them more secure and resilient."[23] FBI Director James B. Comey recognized that "private sector companies . . . possess the information, the expertise and the knowledge to address cyber-intrusions."[24] Mandates will not "enable technical innovation," nor will they "account for organizational differences" as the Executive Order intends.[25] As explained,[26] flexibility is key because standardization of solutions can stunt responses to dynamic and evolving threats, and provide a roadmap for bad actors to focus attacks. Industry must be free to innovate and address the goals of the Framework through their own means.

Specifically, the Executive Order states that the Framework is to "provide guidance that is technology neutral and that enables critical infrastructure sectors to benefit from a competitive market for products and services that meet the standards, methodologies, procedures, and processes developed to address cyber risks," "shall incorporate voluntary consensus standards and industry-based practices," and "shall be consistent with voluntary international standards" when possible.[27] In other contexts, NIST works to "ensure that [its] standards and guidelines do not require specific technological solutions or products, including any specific hardware or software security solutions,"[28] and to also "ensure that [its] standards and guidelines provide for sufficient flexibility to permit alternative solutions to provide equivalent levels of protection for identified information security risks."[29]

To encourage use of the Framework, NIST should promote flexibility and avoid a methodology that might needlessly duplicate an organization's existing processes. Consistent with the Executive Order and NIST's overall policy, industry must retain flexibility to conduct its own prioritization and implementation, including by relying on that which already exists and

---

22 *See infra* Section IV.

23 PPD-21, at 1.

24 Anthony M. Freed, *FBI: Cyber Attacks Will Pose Biggest Threat in Next Decade*, Tripwire.com (Nov. 15, 2013), *available at* http://www.tripwire.com/state-of-security/top-security-stories/fbi-cyber-attacks-will-pose-biggest-threats-next-decade/.

25 Executive Order, at § 7(b).

26 *See* Comments of CTIA – The Wireless Association, Department of Commerce, *Developing a Framework to Improve Critical Infrastructure Cybersecurity*, Docket No. 130208119-3119-01 12 (Apr. 8, 2013) ("CTIA RFI Comments").

27 Executive Order, at §7(b).

28 15 U.S.C. § 278g-3(c)(5).

29 15 U.S.C. § 278g-3(c)(6).

satisfies the goals of the Framework.[30] To that end, NIST should specify that to the extent an organization has or develops a cybersecurity certification program or already has certifications or independent audits of its programs, an organization can leverage such a program under the Framework. *See* CTIA/NCTA/USTA Template Submission at No. 10.

Related to preserving flexibility and encouraging use, NIST should also edit the Framework to clearly state that Categories, Sub-categories, Informative References, and Implementation Tier procedures are provided as tools and are not required or expected for an organization choosing to use the Framework to have satisfactorily done so. There are numerous domestic and international standards and best practices developed by ATIS, IEEE, ANSI, 3GPP and 3GPP2, SCTE, ISO, BITAG, Cloud Security Alliance, and MAAWG, among others, related to cybersecurity.[31] But some of the standards identified, such as NIST SP 800-53 Rev. 4, are government-focused, and NIST should make clear that where such standards or practices are identified, they are provided for government use and not expected or intended for private sector use. *See also infra* at Section IV.C. To that end, the Associations propose that NIST add to the Framework and Appendix A: "<u>While included for completeness, use of government standards by non-government organizations is not required or recommended</u>."[32]

NIST in some places gives a nod to the required flexibility, for example when it states that the Framework Core "is not a checklist."[33] CTIA, NCTA, and USTA propose that NIST make clear that organizations voluntarily using the Framework are free—and encouraged—to choose their own standards and practices which in their view accomplish the objectives of the Framework's Functions and Categories. For example:

- Add to the Framework and Appendix A: *"*<u>Categories, Sub-Categories, and Informative References are provided solely as illustrative tools and are neither intended to constrain use or implementation, nor required for an organization to have satisfactorily used or implemented the Framework</u>*."*
- Change the header for "Informative References" in Appendix A to say: "<u>Illustrative</u> Informative References" and add language: "<u>Any mention of a particular standard, practice, solution, or product as an Informative Reference is for information only; it does not imply NIST recommendation or endorsement, nor does it imply that the standard, practice, solution, or product identified are necessarily the best available for the purpose</u>." This language expands upon language in the "Disclaimer" on page I of the Framework.
- Further revisions are provided in the CTIA/NCTA/USTA Template Submission at No. 84.

---

[30] Some organizations, for example, already have relevant ISO certifications, which should provide organizations comfort that they are adequately using and satisfying the Framework's expectations.

[31] *See* CTIA RFI Comments, at 4-9; Comments of NCTA, Docket No. 130208119-01 9-19; Comments of USTelecom, Docket No. 130208119-01 6-8.

[32] As described below, *infra,* Section IV.C, CTIA, NCTA and USTA further advocate that the NIST SP 800-53 Rev. 4 App. J standards that apply to government agencies be removed from the privacy methodology.

[33] Preliminary Framework, at § 2.1.

One important element of communicating the voluntary nature of the Framework is incorporated in NIST's recent articulation of the emerging consensus on what is meant by "adoption" of the Framework.[34] According to NIST that consensus view is that:

> "An organization adopts the framework when it uses the Cybersecurity Framework as a key part of its systematic process for identifying, assessing, prioritizing, and/or communicating: cybersecurity risks, current approaches and efforts to address those risks, and steps needed to reduce cybersecurity risks as part of its management of the organization's broader risks and priorities."[35]

Although this formulation better promotes flexibility and clarity, CTIA, NCTA, and USTA suggest that NIST revisit, clarify, and deemphasize the "communicating" element. The current proposal does not specify the audience, content, and goals of such communication. As a result, expectations about such communication could hinder use of the Framework. External communication about cybersecurity risks, current approaches and efforts to address those risks, and steps needed to reduce cybersecurity risks threatens to expose information about sensitive, internal deliberative processes and decisions, and it increases the risk of exposing information to cybercriminals and other hackers. Removing or limiting the Framework's expectation about "communicating" will help organizations more readily choose and use the Framework—whether in the context of a future Voluntary Program or otherwise.

Likewise, NIST should encourage use of the Framework by clarifying its references to "information sharing" in the Implementation Tiers and Appendix A,[36] which could be interpreted as expressing a normative expectation regarding the quality and quantity of information sharing. CTIA, NCTA, USTA are acutely aware that cybersecurity defense is enabled best through information sharing between organizations and with the government about potential cyber threats.[37] Organizations and industries presently have different capabilities, needs and risks when it comes to information sharing. Private industry's sharing of information about security processes or vulnerabilities is understandably materially constrained without legislation related to Freedom of Information Act requests, government oversight or enforcement activity, private litigation, civil liability, competitive and antitrust concerns, as well as other concerns. If industry perceives information sharing as a required part of the Framework, or views information sharing expectations as unclear, inflexible or prescriptive, industry could be discouraged from using the Framework. In the end, true improvements in information sharing can only come with legislative action that clarifies and streamlines the process.[38] But to clarify the Framework's references, NIST should explicitly emphasize that information sharing is an optional and flexible aspect of the Framework Core and Tier selection process for organizations that choose to use the Framework, who will have different context for sharing and receiving information.

---

34 NIST, *Update on the Development of the Cybersecurity Framework* 1 (Dec. 4, 2013).

35 *Id.*

36 *See* Preliminary Framework, at 10-11, App. A.

37 *See, infra,* Section IV.A.

38 CTIA, NCTA, and USTA support the Cyber Information Sharing and Protection Act (H.R. 3253), which was reintroduced in the 113th Congress.

C. The Framework Should Be Scalable for Organizations of Different Sizes and Resources.

NIST and the Executive Order both recognize that different types and sizes of organizations have different challenges and abilities. The Executive Order provides that the Framework is to "account for organizational differences," and NIST recognizes that "organizations vary widely in their business models, resources, risk tolerance, [and] approaches to risk management."[39] CTIA, NCTA, and USTA know—from decades of work with different-sized members—that organizations and industries face variable threat landscapes, resources, and cybersecurity needs. Therefore, in response to the Preliminary Framework's inquiry whether it "provide[s] sufficient guidance and resources to aid businesses of all sizes while maintaining flexibility,"[40] the Associations suggest NIST clarify that its Preliminary Framework is a tool to help organizations consider and identify appropriate measures *based on their own risk profiles and needs*.[41] As NIST recognized in its December 4 update, smaller organizations have "special challenges" and "need to develop capabilities to enable use of the framework by smaller organizations that are part of critical infrastructure."

Large and small companies perform cost-benefit analyses for every dollar spent. The Preliminary Framework should provide guidance on how companies should integrate cost-benefit analyses and the Framework. This guidance, in addition to any incentives that are part of the DHS Voluntary Program, would aid small organizations in "cost-effective implementation."[42] Specifically, the guidance would help all companies, large and small, evaluate direct or indirect benefits of various solutions, including the costs associated with technology, people, and process enhancements, and the accompanying reduction in risk. Such guidance also would help the Framework "complement, and . . . not replace, an organization's existing business or cybersecurity risk management process and cybersecurity program."[43]

An effective Framework "must be able to assist organizations in addressing a variety of cybersecurity challenges."[44] To do that, the Framework must not be seen as offering a one-size-fits-all solution and instead must be seen as readily tailored as appropriate for any particular organization, product or service. While this concept will be addressed in part with the foregoing changes, NIST should clarify that different organizations will have different profiles and

---

[39] Preliminary Framework, at 3. Likewise, the Federal Trade Commission has recognized that "reasonable and appropriate" data security solutions "depend on the size and complexity of the business, the nature and scope of its activities, and the sensitivity of the information at issue." *The Data Security and Breach Notification Act of 2010: Hearing on S. 3742 Before the Subcomm. on Consumer Prot., Prod. Safety, & Ins. of the S. Comm. on Commerce, Sci., & Transp.*, 111th Cong. 7 n.22 (Sept. 22, 2010) (prepared statement of FTC).

[40] *Id.*

[41] Along with the release of the Preliminary Framework, NIST released an "alternative presentation of the informative references in Appendix A" for commenters to consider. *See* NIST, *Alternative View: Appendix A* (Oct. 22, 2013), *available at* http://www.nist.gov/itl/upload/alternative-view_appendix-a_framework-core-informative-references.pdf ("Alternative View"). CTIA, NCTA, and USTA support the Appendix A format included in the Preliminary Framework over the Alternate View of Appendix A as a more flexible, clear approach to voluntary use of the Framework.

[42] Preliminary Framework, at i.

[43] *Id.* at 2.

[44] *Id.*

appropriate responses, based on their circumstances, industries, risks and resources. *See* CTIA/NCTA/USTA Template Submission at No. 27.

IV. THE OVERBROAD, COMPLEX, AND OPEN-ENDED PROPOSED PRIVACY METHODOLOGY WILL DISCOURAGE USE OF THE FRAMEWORK AND SHOULD BE REPLACED BY A FLEXIBLE AND STRAIGHTFORWARD INDUSTRY CONSENSUS ALTERNATIVE.

CTIA, NCTA, and USTA support the need to address privacy in the Cybersecurity Framework and believe that tailored privacy safeguards can be integrated into any organization's cybersecurity program. The Associations' members have a long track record of addressing privacy and have programs in place to protect personal information,[45] including in the context of their cybersecurity programs. In addition, telecommunications and cable providers are subject to provisions of the Communications Act that require them to abide by enforceable privacy frameworks that substantively embody many of the Fair Information Practice Principles ("FIPPs").[46] CTIA, NCTA, and USTA members recognize that safeguarding consumer data is a good business practice, and they have strong incentives to earn and maintain consumer trust and loyalty by protecting consumers' data.[47]

CTIA, NCTA, and USTA therefore commend NIST for its efforts to develop privacy guidance to industry in a privacy methodology of the Cybersecurity Framework. The Associations greatly appreciate the extent to which NIST has reached out to and collaborated closely with industry throughout the process of developing the privacy methodology. These groups are concerned, however, that the proposed privacy methodology could discourage industry from using the Cybersecurity Framework because it does not reflect industry consensus; is overbroad, is open-ended and complex, and is overly costly for businesses to put in place. Instead, CTIA, NCTA, and USTA support an Alternative Privacy Methodology recently developed by consensus by a multi-industry group, which encompasses a flexible set of privacy

---

[45] For instance, CTIA developed for its members a Consumer Code for Wireless Service, which requires signatories to abide by a privacy policy that they must make available to the public. CTIA also used the Fair Information Practice Principles to develop the CTIA Best Practices and Guidelines for Location Based Services, which are designed to promote and protect consumer privacy as new location-based services are created and deployed.

[46] Cable system operators are subject to Section 631 of the Communications Act, which requires operators (1) to provide notice to consumers about the personally identifiable information the operators collect, use, disclose, and maintain; (2) to obtain consumers' consent before collecting personally identifiable information, subject to limited exceptions; (3) to give subscribers access to, and the opportunity to correct, personally identifiable information the cable operators have collected; and (4) to take necessary actions to protect the security of personally identifiable information. In addition, Section 222 of the Communications Act requires providers of voice services to comply with privacy protections for customer proprietary network information.

[47] *See e.g.*, Comments of CTIA – The Wireless Association, Department of Commerce, National Telecommunications and Information Administration, *Multistakeholder Process To Develop Consumer Data Privacy Codes of Conduct*, Docket No. 120214135-2135-01, 6-8 (Apr. 2, 2012); Comments of NCTA, National Telecommunications and Information Administration, *Information Privacy and Innovation in the Internet Economy*, Docket No. 101214614-0614-01, at 2, 15-17 (Jan. 28, 2011); Comments of The United States Telecom Association, Docket No. 120214135-2135-01, at 1-5.

guidelines that are focused on privacy issues directly implicated by an organization's cybersecurity measures and that are straightforward for private sector entities to put in place.[48]

A. The Scope of the Proposed Privacy Methodology Is Too Broad and Should Be Limited to Privacy Impacts From Cybersecurity Measures.

The proposed privacy methodology extends beyond what the Executive Order directed NIST to address in its consideration of privacy because it covers more than just the privacy risks potentially associated with a company's deployment of cybersecurity measures. The Executive Order makes clear that the purpose of the Cybersecurity Framework is to "reduce cyber risks to critical infrastructure."[49] The privacy methodology, which will be part of the Framework, therefore should logically be limited to the privacy issues that arise from organizations' efforts to protect the cybersecurity of critical infrastructure. Extending its scope and application beyond this purpose would run the risk of conflicting with existing privacy practices and regulations applicable to organizations' activities in other spheres.

In many places, the proposed privacy methodology extends broadly to address privacy issues beyond those associated with efforts to protect cybersecurity. For instance, the methodologies for "Information Protection Processes and Procedures" direct companies to "[s]ecurely dispose of, de-identify, or anonymize PII that is no longer needed" and to "[r]egularly audit stored PII and the need for its retention."[50] The Cybersecurity Framework, however, is an inappropriate vehicle through which to establish comprehensive privacy standards.

In addition, the proposed privacy methodology covers both (1) personal information that is the target of cyber attacks, *and* (2) personal information that is collaterally affected by industry's protective cybersecurity activities. For instance, the privacy methodology for "Risk Assessment" describes personal information as a potential target: "PII may be targeted as the primary commodity of value or … as a means to access other assets within the organization."[51] The privacy methodology for "Security Continuous Monitoring," on the other hand, describes personal information that could be collaterally affected by cybersecurity measures: "When performing monitoring that involves individuals or PII, regularly evaluate the effectiveness of procedures and tailor the scope to produce minimally intrusive methods of monitoring."[52]

CTIA, NCTA, and USTA agree that the Cybersecurity Framework should address security of different types information, including certain personal information, that could compromise the critical infrastructure. Personal information that is part of the critical infrastructure and that is the *target* of malicious cyber activity should be addressed in the

---

[48] Alternative Privacy Methodology to Protect Privacy for a Cybersecurity Program, attached to letter from Harriet Pearson, Hogan Lovells US LLP to Adam Sedgewick, Information Technology Laboratory, National Institute of Standards and Technology (Dec. 5, 2013), *available at* http://csrc.nist.gov/cyberframework/framework_comments/20131205_harriet_pearson_hoganlovells.pdf ("Alternative Privacy Methodology").

[49] Executive Order, § 7(b).

[50] Preliminary Framework, Appendix B, at 30-31.

[51] Preliminary Framework, Appendix B, at 29.

[52] Preliminary Framework, Appendix B, at 31.

Cybersecurity Framework Core, and not in the privacy methodology. In the Framework Core, personal information should be treated the same any other potentially valuable asset (such as intellectual property) that is at risk of cyber attack. Consistent with the foregoing and to avoid confusion caused by duplication and potential conflicting directions, the Framework Core need not and should not make specific references to privacy beyond data security.

By contrast, the privacy methodology should be limited to only address personal information that may be *collaterally affected* by a company's cybersecurity measures. Accordingly, NIST should narrow the scope of the privacy methodology to address those unique privacy risks associated with critical infrastructure companies' efforts to protect cybersecurity, such as monitoring, information sharing, and access to information.

B. The Proposed Privacy Methodology Does Not Provide Clear and Practical Privacy-Protective Processes.

The proposed privacy methodology in many respects is too vague to provide meaningful and practical guidance to those individuals in critical infrastructure companies who may be putting in place the Cybersecurity Framework. CTIA, NCTA, and USTA urge NIST to revise the methodology to describe the sort of processes that companies using the Framework should put in place to identify, prevent, and mitigate privacy risks associated with cybersecurity activities. For instance, the proposed privacy methodology for "Access Control" states that, entities should "[l]imit the use and disclosure of personally identifiable information to the minimum amount necessary to provide access to applications, services, and facilities,"[53] but compliance with that goal is complex, subjective, and not easily evaluated, especially because there is no industry consensus standard for doing so. In addition, this methodology does not allow companies sufficient flexibility and risks undermining cybersecurity. It could preclude, for instance, the use of some access controls, such as biometric authentication or two-factor authentication, that require users to provide *more* personal information, but are stronger than other authentication tools that require users to provide *less* personal information.

A better approach would set up *processes* by which entities would give appropriate consideration to the privacy implications associated with relevant aspects of their cybersecurity programs. For instance, the methodology for controlling access to information could be modified to provide as follows: "Steps are taken to identify and address the privacy implications of access control measures to the extent that they involve collection or use of protected information relating to identifiable individuals."[54] This approach would ensure companies put in place processes to curtail data use and disclosure and, at the same time, give entities the flexibility to use measures that complement their cybersecurity programs, business processes, risk assessments, and existing privacy programs.

CTIA, NCTA and USTA therefore urge NIST to design the privacy methodology to encourage entities choosing to use the Framework to select and employ governance processes and privacy policies, which trained individuals would put in place and which would foster

---

53 *Id.* at 30.

54 Alternative Privacy Methodology, at 4.

communication and cooperation between individuals who manage and oversee the entity's cybersecurity program and privacy program.

C. The Proposed Privacy Methodology Improperly Relies Heavily on NIST Special Publication 800-53, Which Was Designed for Federal Agencies, Not for the Private Sector.

The proposed privacy methodology directs companies to numerous provisions in NIST Special Publication 800-53: *Security and Privacy Controls for Federal Information Systems and Organizations* ("SP 800-53"), which NIST developed to be a "catalog of security and privacy controls **for federal information systems and organizations**," and include provisions that are not necessarily applicable for the private sector.[55] SP 800-53 makes clear that its privacy controls are "intended to address the privacy needs of **federal agencies**" and to help them "satisfy[] **federal privacy requirements**."[56] These requirements include compliance with the Privacy Act of 1974 (the "Privacy Act"), the E-Government Act of 2002, Executive Orders, and Office of Management and Budget ("OMB") policies and directives.[57] Communications companies are already subject to a variety of legal and regulatory requirements designed to protect personal information and safeguard the privacy of customer data and communications. Layering onto these existing privacy regimes a separate set of privacy measures that have been devised for federal agencies that are not subject to the existing private sector privacy legal and regulatory regimes will inhibit use of the Framework while providing little incremental benefit to privacy.

SP 800-53 assists federal agencies in fulfilling their unique statutory and regulatory responsibilities by correlating privacy controls directly to particular statutory provisions of the Privacy Act and OMB memoranda. For instance, SP 800-53 includes a privacy control called "accounting of disclosures" (AR-8) which helps federal agencies to comply with their statutory obligation to account for disclosures of records under the Privacy Act, with appropriate exceptions for disclosures made pursuant to the Freedom of Information Act or to law enforcement agencies.[58] SP 800-53 also contains a privacy control for "individual access" (IP-2), which directs federal agencies to publish "rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records" and to adhere to "Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests."[59] In addition, the privacy control for "authority to collect" (AP-1) refers to a statutory provision that requires federal agencies to cite their authority (either under a statute or executive order by the President) to collect the personal information sought.[60]

---

55 SP 800-53, at iii (emphasis added).

56 SP 800-53, at xi (emphasis added.).

57 SP 800-53, Appendix J, at J-2 (stating that the "privacy controls in this appendix are based on the Fair Information Practice Principles (FIPPs) embodied in the Privacy Act of 1974, Section 208 of the E-Government Act of 2002, and Office of Management and Budget (OMB) policies").

58 SP 800-53, Appendix J, at J-11.

59 SP 800-53, Appendix J, at J-18.

60 SP 800-53, Appendix J, at J-6.

The Privacy Act, which encompasses the full set of FIPPs, was designed to address the unique privacy and civil liberties concerns that arise when the government collects and uses information about its citizens.[61] It reflects a unique set of cost-benefit tradeoffs that are justifiable because it limits government action. Application of SP 800-53 to the private sector is therefore largely inapposite. Indeed, NIST's inclusion of SP 800-53 references in the privacy methodology is at odds with the approach the White House took when it issued its report, titled *Consumer Data Privacy in a Networked World* (2012), which provided consumer data privacy guidance to the private sector. The White House report expressly acknowledged the inapplicability of the Privacy Act and OMB guidance to the private sector:

> This framework is concerned solely with how private-sector entities handle personal data in commercial settings. A separate set of constitutional and statutory protections apply to the government's access to data that is in the possession of private parties. In addition, the Privacy Act of 1974 . . . and implementing guidance from the Office of Management and Budget . . . , govern the Federal government's handling of personally identifiable information. Both of these areas are beyond the scope of this document.[62]

The privacy controls embodied in SP 800-53 would be confusing and costly for companies in the private sector to put in place. Companies would expend unnecessary resources trying to transpose these controls, which are intended primarily for federal government agencies, into protocols suitable for private industry. Ultimately, consumers would bear the increased costs that would result, even though they are unlikely to receive any discernible benefit from the application of these particularized principles. Limiting the privacy methodology to tailored privacy processes that are flexible enough to adapt to companies' actual business practices will allow companies to focus on those privacy issues actually implicated by their protective cybersecurity measures.

D. Civil Liberties Are an Appropriate Consideration for Governmental Entities, but Generally Would Not Be Applicable to the Private Sector.

The privacy methodology states that it addresses both privacy and civil liberties associated with cybersecurity activities. To the extent that civil liberties requirements would apply to private sector actors—when, for example, a private sector entity contracts with the federal government to provide specific services—they would be addressed through contracts

---

[61] The purpose of the Privacy Act "is to balance the government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy stemming from **federal agencies'** collection, maintenance, use, and disclosure of personal information about them." *Overview of the Privacy Act of 1974*, U.S. Department of Justice 4 (2012) (emphasis added) *available at* http://www.justice.gov/opcl/1974privacyact-overview.htm. Congress passed the Privacy Act in an effort to "curb[] the illegal surveillance and investigation of individuals by **federal agencies** that had been exposed during the Watergate scandal." *Id.* (emphasis added). Congress also was "concerned with potential abuses presented by the **government's increasing use** of computers to store and retrieve personal data by means of a universal identifier – such as an individual's social security number." *Id.* (emphasis added).

[62] *See* The White House, *Consumer Data Privacy in a Networked World* 5, n.1 (Feb. 2012) *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

between the government agency and the private sector entity. As a general matter, however, private sector entities not so constrained will address protections for the free flow of ideas across their networks through different, existing methods.

As explained above, SP 800-53 references laws and practices that govern the *federal government's* use of personal data, which reflect—as they must—important civil liberties issues under the U.S. Constitution. The privacy methodology for Framework Core Function "Respond" and Category "Mitigation," for instance, reflects these concerns: "When considering methods of incident containment, assess the impact on individuals' privacy and civil liberties, particularly for containment methods that may involve the closure of public communication or data transmission systems. Provide transparency concerning such methods." This is an appropriate consideration for federal agencies, which must weigh important constitutional issues when determining whether to urge a company to shut down a network to interrupt or prevent an attack. By their nature, however, private sector entities must weigh different considerations.

In the private sector, market forces provide communications companies with strong incentives both to secure their networks and not interrupt their service. Moreover, it is not clear exactly which civil liberties companies are expected to work to protect. Some entities offer services that are vital to free expression. Other entities may not provide services that users rely on to voice an opinion, but are subject to common carrier obligations.

E. A Better Approach Would Provide a Tailored, Flexible, and Process-Oriented Privacy Methodology.

The privacy methodology's detailed and broad requirements, and its references to SP 800-53, if construed as being required or preferred, would impose expectations and burdens on industry that do not represent industry consensus and that would discourage use of the Framework. NIST should consider instead a privacy methodology that (1) focuses on the privacy issues directly associated with protective cybersecurity measures, instead of a comprehensive framework for the handling of personal information that overlaps in places with Appendix A; (2) complements the Framework Core by allowing companies to develop processes that can be integrated into existing business operations; (3) is designed to apply to private industry; and (4) is straightforward and cost-effective for industry to use. Private sector entities would be much more likely to use the Cybersecurity Framework if the privacy methodology took this tailored, flexible, and process-oriented approach.

To that end, CTIA, NCTA and USTA encourage NIST to adopt the Alternative Privacy Methodology submitted to NIST on December 5, which the Associations helped to develop in conjunction with other critical infrastructure sectors and which embodies the principles outlined above.[63] The Alternative Privacy Methodology addresses the collection and use of "protected information" related to an organization's cybersecurity activities.[64] It does not apply to commercial data protection outside of the cybersecurity context. The Alternative Privacy

[63] Alternative Privacy Methodology.

[64] *Id.* at 4. The Alternative Privacy Methodology defines "protected information" as "personal information that (i) is subject to security breach notification requirements, (ii) an organization is restricted by law from disclosing, (iii) an organization is required by law to secure against unauthorized access, or (iv) an organization voluntarily so designates." *Id.*

Methodology provides clear guidance to companies, instructing them to (1) consider the privacy implications of cybersecurity programs as part of their overall governance of cybersecurity risk; (2) include privacy considerations in their cybersecurity awareness and training programs; and (3) put processes in place to protect privacy in the context of the organization's access control mechanisms, cybersecurity monitoring activities, and cybersecurity-related information sharing.[65] This focused and flexible methodology reflects consensus private sector standards, is clear and understandable for the private sector to use, and is more likely to incentivize use of the Cybersecurity Framework.

[65] *Id*. Although CTIA, NCTA, and USTA believe that the Cybersecurity Framework should not impose expectations regarding information sharing, these groups recognize that organizations can and will share cybersecurity threat information at their discretion, and when they do, they should consider the privacy implications of such sharing.

V. CONCLUSION

CTIA, NCTA, and USTA commend NIST for its work to date on this project. The communications industry is pleased to be able to share its perspective on the Framework's contents and use, and to offer these suggestions to improve and clarify the document. With these changes, the Associations are optimistic that the Framework can become an important resource that will help large and small organizations evaluate and improve their cybersecurity posture.

Respectfully Submitted,

CTIA- The Wireless Association
National Cable & Telecommunications Association
U.S. Telecom Association

By:
/Michael Altschul/
/John Marinho/
/Debbie Matties/

CTIA- The Wireless Association
Michael Altschul, Senior Vice President, General Counsel
John Marinho, Vice President, Cybersecurity
Debbie Matties, Vice President, Privacy

By:
/Rick Chessen/
/Loretta Polk/
/Matt Tooley/

National Cable & Telecommunications Association
Rick Chessen, Senior Vice President, Law and Regulatory Policy
Loretta Polk, Vice President and Associate General Counsel
Matt Tooley, Senior Director, Broadband Technology

By:
/Jon Banks/
/Robert Mayer/

US Telecom Association
Jon Banks, Senior Vice President, Law and Policy
Robert Mayer, Vice-President, Industry and State Affairs

December 13, 2013