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

In the Matter of	)	
	)	
Developing a Privacy Framework	)	NIST Request for Information
	)	Docket No. 181101997-8997-01
	)	

COMMENTS OF CTIA

Thomas C. Power
Senior Vice President and General Counsel

Melanie K. Tiano
Director, Cybersecurity and Privacy

CTIA

www.ctia.org

January 14, 2019

TABLE OF CONTENTS

Page

I. INTRODUCTION AND SUMMARY

CTIA[1] appreciates the opportunity to engage with the National Institute of Standards and Technology ("NIST") on this important Privacy Framework effort. NIST's *Request for Information* (the "RFI")[2] marks a significant first step in seeking stakeholder input. CTIA applauds NIST's leadership in developing a "framework that can be used to improve organizations' management of privacy risk for individuals arising from the collection, storage, use, and sharing of their information."[3] A voluntary Privacy Framework could be a valuable tool to help organizations understand and manage privacy-related risks. It may be most valuable for organizations who have not developed a robust approach to privacy.

There is significant work ongoing throughout the government related to consumer privacy, and CTIA is engaged. CTIA filed comments on the Administration's consideration of privacy principles,[4] is engaged with the Federal Trade Commission, and is also engaged with Congress as they explore these issues. CTIA encourages NIST to also coordinate with others throughout the Federal government, including those at NTIA, the FTC, and Congress, who are actively working on these issues.

Safeguarding consumer privacy is a top priority for the wireless industry, which has long embraced a leadership role. Companies have incentives to develop robust privacy programs and

---

[1] CTIA® (www.ctia.org) represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem that enable Americans to lead a 21st-century connected life. The association's members include wireless carriers, device manufacturers, suppliers as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. The association also coordinates the industry's voluntary best practices, hosts educational events that promote the wireless industry, and co-produces the industry's leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

[2] *Developing a Privacy Framework*, Request for Information, Docket No. 181101997-8997-01, 83 Fed. Reg. 56824 (Nov. 14, 2018) ("NIST RFI").

[3] *Id.* at 56824.

[4] *See* Comments of CTIA, NTIA Docket No. 180821780-8780-01 (filed Nov. 9, 2018), https://www.ntia.doc.gov/files/ntia/publications/181109_ntia_rfc_comments_of_ctia.pdf; *Developing the Administration's Approach to Consumer Privacy*, Request for Public Comments, NTIA Docket No. 180821780-8780-01, 83 Fed. Reg. 48600 (Sept. 26, 2018) ("NTIA RFC").

practices to maintain consumer trust, which is key for the continued growth of the mobile ecosystem.

CTIA members incorporate privacy protections into their products and services. Examples abound. CTIA and wireless carriers committed publicly to adhere to core principles to protect customers' privacy online, known as the ISP Privacy Principles.[5] These principles include transparency, choice, security, and data breach notification. CTIA and wireless carriers have also made a voluntary commitment to uphold the Consumer Code for Wireless Service—twelve principles and practices to help consumers make informed decisions when selecting wireless services.[6] Carriers conduct privacy impact assessments as a matter of practice and provide consumers information about how customers' data is protected and what choices customers can make about their data.[7]

CTIA supports NIST's overall approach to the Privacy Framework and offers suggestions to support industry efforts. Specifically, CTIA:

- Asks NIST to use the Privacy Framework to facilitate and encourage innovative and beneficial uses of data.
- Urges NIST not to engage in policy making or make value judgments in this Privacy Framework process. NIST's goal should be to create a practical tool for organizations to use regardless of jurisdiction or applicable legal regime.
- Applauds NIST for modeling the Privacy Framework process after the successful Cybersecurity Framework by creating a collaborative and consensus-based process, but urges NIST to take care in using the Cybersecurity Framework as a model for its work product given some fundamental differences between privacy and cybersecurity.
- Supports the "attributes" identified by NIST in the RFI for the Privacy Framework.

[5] CTIA et al., *ISP Privacy Principles* (Jan. 27, 2017), https://api.ctia.org/docs/default-source/default-document-library/final---protecting-consumer-privacy-online.pdf.
[6] *See* CTIA, *Consumer Code for Wireless Service*, https://www.ctia.org/the-wireless-industry/industry-commitments/consumer-code-for-wireless-service (last visited Dec. 19, 2018).
[7] *See, e.g.*, Meredith Atwell Baker, *Your Mobile Data Remains Safe: Wireless Privacy Protections*, CTIA Blog (Apr. 3, 2017), https://www.ctia.org/news/mobile-data-safe-wireless-privacy-protections.

- Encourages NIST to take into account the key differences between the federal government and the private sector when it comes to privacy, and to develop a flexible approach that encompasses both.

- Suggests a set of value-agnostic questions that a general Privacy Framework could use to help organizations, regardless of privacy posture, to assess and/or improve their management of privacy. This list draws upon established methods for identifying, managing, and responding to privacy risks.

II. THE PRIVACY FRAMEWORK MUST FACILITATE AND ENCOURAGE INNOVATIVE AND BENEFICIAL USES OF DATA.

The collection and use of data enables products and services that can transform lives. For example, in the healthcare industry, wearable devices and consumer engagement through mobile health apps allow medical professionals to treat patients based on their established health baseline rather than a moment in time.[8] Developments in artificial intelligence ("AI") and machine learning can help farmers make informed decisions on when to plant, water, and harvest based on data collected about rainfall, temperatures, windspeed, soil PH, and more.[9] These are just a few examples.

Data-driven technologies such as advanced analytics, machine learning, and AI hold great promise within the wireless sector. These technologies can increase data security, including by use of biometric data for authentication. Data-driven technologies contribute to fraud detection and prevention and real-time threat detection, among other things.[10] These data-driven technologies will be critical to next-generation wireless networks like 5G.

> Beyond just security, AI will be key to all areas of network operations[.] . . . As [providers] prepare for 5G, the ones who will to be successful over the long term will focus on introducing advanced network operations and customer experience systems into the network. The increased number of network elements, coupled with

[8] *See* Eric Wicklund, *An mHealth Wearable Helps Cedars-Sinai Doctors Manage Patient Care*, mHealthIntelligence.com (Jan. 18, 2018), https://mhealthintelligence.com/news/an-mhealth-wearable-helps-cedars-sinai-doctors-manage-patient-care.
[9] *See* The Yield Technology Solutions, https://www.theyield.com/ (last visited Dec. 19, 2018).
[10] *See, e.g.*, Sean Kinney, *AI and 5G go hand-in-hand for network operations*, RCR Wireless News (Aug. 3, 2018), https://www.rcrwireless.com/20180803/wireless/ai-5g-network-operations-tag17.

the increased number of devices connected, will make it nearly impossible to run a 5G network without the assistance of AI-driven analytics.[11]

CTIA is encouraged that NIST has committed to developing a Privacy Framework "in a manner consistent with its mission to promote U.S. innovation and industrial competitiveness."[12] However, well-intentioned policymakers can take action that inadvertently chills innovation and competition. As Federal Communications Commission ("FCC") Chairman Ajit Pai said at a forum on AI and machine learning: "History tells us that new technologies will evolve in ways that people don't anticipate and that early intervention can forestall or even foreclose certain paths to innovation. This makes it foolish and counterproductive for government to micromanage—or more accurately, try to micromanage—the evolution of these technologies."[13]

Critically, the Privacy Framework should support innovative and beneficial uses of data with appropriate safeguards. The NIST Privacy Framework can help foster the continued use of data for the development of technologies like AI, which depend on the collection and analysis of vast amounts of data, and for research. NIST should recognize and promote tools such as de-identification, which facilitates beneficial uses of data while protecting privacy. In addition, the Privacy Framework can support deployment of new, data-based technologies and strengthen consumer trust.

[11] *Id.*
[12] *NIST RFI* at 56824.
[13] Ajit Pai, Chairman, Fed. Commc'ns Comm'n, Remarks at the FCC Forum on Artificial Intelligence and Machine Learning, at 1 (Nov. 30, 2018), https://docs.fcc.gov/public/attachments/DOC-355344A1.pdf.

III. NIST'S PRIVACY FRAMEWORK SHOULD MEANINGFULLY SUPPORT INDUSTRY'S EFFORTS TO MITIGATE PRIVACY RISKS.

A. The Privacy Framework must be policy neutral for it to be widely adopted and effective.

NIST should not engage in policy making, establish substantive expectations, or make value judgments in the Privacy Framework process. NIST should focus on producing a practical tool for organizations, which is, as NIST says, "compatible with and support[s] organizations' ability to operate under applicable domestic and international legal or regulatory regimes."[14]

Policy decisions about risks, harms, and what data to protect should be made by Congress, with assistance from the FTC and NTIA. In testimony before the Senate Subcommittee on Consumer Protection, the FTC reiterated its request for Congress to enact privacy legislation that addresses consumers' legitimate concerns, provides clarity to businesses, and retains flexibility to enable competition and innovation. The agency emphasized that this "will involve difficult value judgments and tradeoffs that are appropriately left to Congress."[15]

There are processes underway at the FTC and NTIA, in which CTIA has been involved. These include FTC hearings on consumer privacy, "the first comprehensive re-examination of the FTC's approach to consumer privacy since 2012,"[16] and NTIA's effort to develop the Administration's approach to consumer privacy.[17] NIST's Privacy Framework should be coordinated with these proceedings. Importantly, NIST should be careful to refrain from establishing substantive expectations that are being considered in those proceedings for two

---

[14] *NIST RFI* at 56825.
[15] *Oversight of the Fed. Trade Comm'n: Hearing Before the Subcomm. on Consumer Prot., Prod. Safety, Ins., & Data Sec. of the S. Comm. on Commerce, Sci., & Transp.*, 115th Cong. 9 (2018) (prepared statement of the Fed. Trade Comm'n), https://www.ftc.gov/system/files/documents/public_statements/1423835/p180101_commission_testimony_re_oversight_senate_11272018_0.pdf.
[16] Press Release, FTC, *FTC Announces Sessions on Consumer Privacy and Data Security as Part of its Hearings on Competition and Consumer Protection in the 21st Century* (Oct. 26, 2018), https://www.ftc.gov/news-events/press-releases/2018/10/ftc-announces-sessions-consumer-privacy-data-security-part-its.
[17] *See NTIA RFC.*

primary reasons: *first*, the Privacy Framework should not reflect the individual policy decisions of any single regime, and *second*, NIST should not include policy content in its Privacy Framework because doing so could contradict or be inconsistent with other U.S. agency determinations or Congressional judgments, and instead should focus on creating a flexible outcome-based framework that can be adapted to whichever privacy framework or substantive privacy requirements are developed by Congress or expert agencies. A few of the questions and definitions included in the RFI help to illustrate this point. For example:

- **Privacy Risk:** The RFI asks about how organizations define privacy risk. Risks will vary based on context and applicable legal regimes. As CTIA noted to NTIA, the definition of "privacy risk" is critical to a risk-based approach.[18] This threshold definition is best defined by policymakers and is currently being considered by NTIA and FTC. NIST should not attempt to define privacy risk in the Privacy Framework; leaving it to organizations will make the Framework more broadly useful.

- **Privacy Harm:** Similarly, NIST should not define "privacy harm," which is an important policy decision. In NISTIR 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems*,[19] NIST explored the topic of defining "privacy problems" in federal systems. While that work can help to inform policymakers, it should not be incorporated into the Privacy Framework. Congress, NTIA and the FTC are all looking at privacy harms.[20]

- **PII:** In the RFI, NIST uses the definition of personally identifiable information ("PII") from Office of Management and Budget Circular A–130, which defines PII as "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual."[21] CTIA urges NIST not to incorporate this definition, because the approach used by OMB for federal government entities should not be used in a regime-neutral and generally applicable Privacy Framework. There are different threshold definitions for covered data under different regimes—for example, "personal data" under The European Union's General Data Protection Regulation ("GDPR") is different from "personal information" under the California Consumer Privacy Act ("CCPA"), which is different

[18] *See* Comments of CTIA, NTIA Docket No. 180821780-8780-01 (filed Nov. 9, 2018), https://www.ntia.doc.gov/files/ntia/publications/181109_ntia_rfc_comments_of_ctia.pdf.
[19] NIST, Internal Report 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems*, 9 (Jan. 2017), https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf.
[20] *See, e.g.*, FTC, BE & BCP Staff Perspective, *FTC Informational Injury Workshop* (Oct. 2018), https://www.ftc.gov/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective; FTC, *Hearings on Competition and Consumer Protection in the 21st Century*, https://www.ftc.gov/policy/hearings-competition-consumer-protection (last visited Dec. 19, 2018) (Hearing #10, Consumer Privacy).
[21] *NIST RFI* at 56824 n.3.

from "customer proprietary network information" or "CPNI" under the Communications Act. NIST should not choose one, as these threshold definitions for covered data vary across regimes, and may change as federal policy evolves.

B. NIST is rightly building on its success in developing the Cybersecurity Framework to facilitate this process, but should take care to recognize key differences between privacy and cybersecurity in drawing on the Cybersecurity Framework.

CTIA supports NIST's decision to "model the approach for the Privacy Framework on the successful, open, transparent, and collaborative approach used to develop the [Cybersecurity Framework]."[22] The process that lead to the development of the Cybersecurity Framework is a cornerstone of its success. CTIA was heavily involved in the Cybersecurity Framework, Version 1.0 and Version 1.1.

It took one year from the release of the first *Request for Information* to develop Version 1.0 of the Cybersecurity Framework. As captured in the attached timeline, NIST engaged with stakeholders early and often,[23] holding five workshops, releasing three formal requests for public comment, and engaging in informal outreach to facilitate broad participation, all before the release of Cybersecurity Framework Version 1.0.[24]

CTIA encourages NIST to take the same ample time to collaboratively develop a Privacy Framework. CTIA appreciates NIST's commitment to a framework that is "consensus-driven and developed and updated through an open, transparent process."[25] Like the Cybersecurity

[22] *Id.* at 56825.
[23] *See* Appendix, *Timeline of the NIST Cybersecurity Framework Process*.
[24] *See id.*
[25] *NIST RFI* at 56825.

Framework, the Privacy Framework will be most effective by leveraging the expertise and experiences of all interested stakeholders.

However, while the *process* used to develop the Cybersecurity Framework is the right approach, NIST should be careful to recognize the key differences between privacy and cybersecurity before adopting substance. It is critical that NIST recognize that privacy risk management concepts are distinct from those in the cybersecurity context. Cybersecurity risk management tools are more plentiful and more mature than privacy risk management tools. This means candidates for "informative references" for the Privacy Framework may be more variable and less useful. In addition, cybersecurity outcomes tend to be more objective, while privacy goals tend to be value-based and variable.[26] NIST should account for these differences in creating a Privacy Framework that is policy neutral.

CTIA agrees that privacy risk management overlaps with and reinforces security. Safeguards such as encryption, pseudonymization, de-identification, enforceable codes of conduct, and security protections enable innovative and beneficial uses of data, while reducing risk of misuse or harm to individuals.

This relationship between protecting consumer privacy and facilitating new, innovative, and beneficial uses of data, as discussed above, requires that the Privacy Framework reflect a somewhat different approach from the Cybersecurity Framework. While the Cybersecurity Framework focuses on risks and threats, the Privacy Framework should focus on facilitating the

[26] *See* NIST, *NIST Roadmap for Improving Critical Infrastructure Cybersecurity*, at 8-9 (Feb. 12, 2014), https://www.nist.gov/sites/default/files/roadmap-021214.pdf ("A key challenge for privacy has been the difficulty in reaching consensus on definition and scope management, given its nature of being context-dependent and relatively subjective. . . . Although research is being conducted in the public and private sectors to improve current privacy practices, many gaps remain.").

adoption of reasonable privacy protections without hindering development of new technologies. CTIA urges NIST to consider and incorporate this distinction, which is not reflected in the RFI.

C. NIST is correct to strive for the same attributes in the Privacy Framework that help to make the Cybersecurity Framework successful.

NIST's Cybersecurity Framework has been widely used in the private and public sectors, as well as internationally.[27] In addition to the process that created it, the Cybersecurity Framework's success is due to its attributes: "[t]he voluntary, risk-based, flexible, repeatable, and cost-effective approach of the Framework helps those who use the Framework to manage cybersecurity risk."[28] NIST's Privacy Framework can help organizations enhance efforts to address privacy. As with the Cybersecurity Framework, NIST should not adopt a one-size-fits-all approach, nor should it promote a checklist mentality. NIST is right to promote "a prioritized, flexible, risk-based, outcome-based, and cost-effective approach that can be compatible with existing legal and regulatory regimes in order to be the most useful to organizations and enable widespread adoption."[29]

CTIA supports the seven attributes identified in the RFI, specifically, that the Privacy Framework should: (1) be "[c]onsensus-driven and developed and updated through an open, transparent process;" (2) use "[c]ommon and accessible language;" (3) be "[a]daptable to many different organizations, technologies, lifecycle phases, sectors, and uses;" (4) be "[r]isk-based, outcome-based, voluntary, and non-prescriptive;" (5) be "[r]eadily useable as part of any enterprise's broader risk management strategy and processes;" (6) be "[c]ompatible with or may

---

[27] NIST, Cybersecurity Framework, Perspectives on the Framework: International Perspectives, https://www.nist.gov/cyberframework/perspectives#international (last visited Dec. 19, 2018).
[28] *Bolstering the Government's Cybersecurity: Assessing the Risk of Kaspersky Lab Products to the Federal Government Hearing Before the Subcomm. on Oversight of the H. Comm. on Science, Space, & Tech.*, 115th Cong. 3 (2017), https://science.house.gov/sites/republicans.science.house.gov/files/documents/HHRG-115-SY21-WState-DDodson-20171025.PDF (testimony of Donna Dodson, Chief Cybersecurity Advisor and Director of NCCoE, NIST).
[29] *NIST RFI* at 56824.

be paired with other privacy approaches; and (7) be "[a] living document."[30] Three particular attributes are critical.

1. *Adaptable to Many Different Organizations, Technologies, Lifecycle Phases, Sectors, and Uses.*

Flexibility is central to the success of a Privacy Framework. Privacy risks vary by sector, size, and sophistication of individual companies. The Privacy Framework should build in flexibility to enable organizations of all types to address privacy, as the Cybersecurity Framework gives organizations the flexibility to assess and mitigate their own cyber risks. This approach recognizes that organizations offer diverse products and services to consumers, each with varying use cases and varying benefits to consumers.

Emphasis on flexibility is common across Administration privacy efforts. NTIA recognized the importance of flexibility in its *Request for Comment* on privacy principles: "The Administration is proposing that these outcomes be operationalized through a risk-management approach, one that affords organizations flexibility and innovation in how to achieve these outcomes."[31] Likewise, the FTC recently noted the "need to preserve flexibility to address complex and evolving issues related to consumer privacy and data collection, and broader impacts on innovation and competition."[32] As part of this flexibility, the Privacy Framework should be technology- and sector-neutral, to reflect that data is collected and used in different ways by different types of companies for various beneficial uses. A technology-neutral approach will apply uniformly and help facilitate adoption of the Privacy Framework.

---

[30] *Id.* at 56825.
[31] *NTIA RFC* at 48601.
[32] Comments of Federal Trade Commission Staff, NTIA Docket No. 180821780–8780–01, at 19 (filed Nov. 9, 2018), https://www.ntia.doc.gov/files/ntia/publications/federal_trade_commission_staff_comment_to_ntia_11.9.2018.pdf ("FTC Comments").

2. *Risk-based, outcome-based, voluntary, and non-prescriptive.*

These attributes are key to NIST's cybersecurity work, and CTIA is encouraged that NIST sees them as minimum attributes for the Privacy Framework.

Risk- and outcome-based. CTIA members have been using risk management practices for decades. Risk management is a critical concept, regularly examined and refined by NIST,[33] and it should be at the heart of the Privacy Framework. As NIST explains elsewhere, a "risk-based approach . . . considers effectiveness, efficiency, and constraints due to applicable laws, directives, Executive Orders, policies, standards, or regulations."[34] A risk- and outcome-based approach will be broad enough to accommodate the many variables affecting organizations' privacy risk management and enable positive privacy outcomes—encouraging organizations to utilize strategies most appropriate for them. This approach will encourage wide use of the Privacy Framework across the diversity of organizations in the United States and make it useful abroad, as the Cybersecurity Framework has been.

Risk management is a focus of NTIA and FTC work, as well. NTIA says that risk management "is the core of this Administration's approach, as it provides the flexibility to encourage innovation in business models and privacy tools, while focusing on potential consumer harm and maximizing privacy outcomes."[35] And "a risk-based approach is in the FTC's institutional DNA."[36]

---

[33] *See* NIST, *Computer Security Resource Center: Risk Management*, https://csrc.nist.gov/projects/risk-management/risk-management-framework-(rmf)-overview (last visited Dec. 19, 2018); NIST, Draft SP 800-37 (Rev. 2), Final Public Draft, *Risk Management Framework for Information Systems and Organization: A System Life Cycle Approach for Security and Privacy* (Oct. 2018).
[34] NIST, *Computer Security Resource Center: Risk Management*, https://csrc.nist.gov/projects/risk-management/risk-management-framework-(rmf)-overview (last visited Dec. 19, 2018).
[35] *NTIA RFC* at 48602.
[36] *FTC Comments* at 11.

Voluntary. This attribute is important to provide maximum effectiveness and flexibility, encourage widespread use, and facilitate innovation. NIST should include explicit language about the voluntary nature of the Privacy Framework. NIST should refrain from using language that might imply that the Privacy Framework's guidance is not voluntary.

Non-Prescriptive. Non-prescriptive guidance better facilitates privacy protections. It encourages organizations to adopt risk management strategies that provide meaningful outcomes, as opposed to undertaking a mere "check-the-box" compliance exercise. Further, establishing prescriptive requirements would also put NIST in the position of establishing policy or putting a thumb on the scale of a particular policy approach, neither of which would be appropriate.

The Cybersecurity Framework points organizations to substantive and technical cybersecurity guidance and best practices in informative references.[37] This provides users a menu of options from which to choose, and not a fixed list of requirements. The Privacy Framework should take the same approach. Privacy standards and approaches that could be used as informative references include:

- ISO/PC 317—Consumer protection: privacy by design for consumer goods and services (under development).[38]
- The FTC's 2012 Privacy Report, *Protecting Consumer Privacy in an Era of rapid Change* and other FTC guidance.[39]

[37] *See* NIST, *Cybersecurity Framework: Questions and Answers*, https://www.nist.gov/cyberframework/questions-and-answers#informative (last visited Dec. 19, 2018) ("Informative References [] show relationships between Framework Functions, Categories, and Subcategories and specific sections of standards, guidelines, and practices common among Framework stakeholders. Informative References illustrate ways to achieve Framework outcomes.").
[38] International Organization for Standardization, *ISO/PC 317, Consumer protection: privacy by design for consumer goods and services*, https://www.iso.org/committee/6935430.html (last visited Dec. 19, 2018).
[39] FTC, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Mar. 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

- ISO/IEC 27000,[40] a suite of standards for securing information assets. This includes ISO/IEC 27001, which provides guidance on information security management systems.

- OECD privacy frameworks, including the Revised Guidelines on the Protection of Privacy and Transborder Flows of Personal Data[41] and guidance from the OECD Going Digital project.[42]

- The European Union's GDPR,[43] establishing a risk-based approach to privacy management. GDPR Article 35 requires data protection impact assessments "taking into account the nature, scope, context and purposes of processing" and with a focus on processing "likely to result in a high risk."[44]

3. *Compatible with or may be paired with other privacy approaches.*

CTIA agrees with NIST's decision to pursue a Privacy Framework that is "compatible with and support[s] organizations' ability to operate under applicable domestic and international legal or regulatory regimes."[45] This neutrality is especially important as companies often operate across international and state borders. By taking a regime-neutral approach, NIST will enable organizations to adopt the Privacy Framework irrespective of jurisdiction. Organizations that operate under the GDPR, Canada's Personal Information Protection and Electronic Documents Act ("PIPEDA"),[46] the CCPA,[47] Section 5 of the Federal Trade Commission Act,[48] or a combination of these or other laws should all be able to utilize the Privacy Framework. Similarly, a regime-neutral Privacy Framework should be usable irrespective of sector-based

[40] International Organization for Standardization, *ISO/IEC 2700 family – Information security management systems*, https://www.iso.org/isoiec-27001-information-security.html (last visited Dec. 19, 2018).
[41] Organization for Economic Cooperation and Development, *The OECD Privacy Framework* (2013), http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.
[42] Organization for Economic Cooperation and Development, *Going Digital*, http://www.oecd.org/going-digital/ (last visited Dec. 19, 2018).
[43] Commission Regulation 2016/679, General Data Protection Regulation, 2016 J.O. (L 119) 1, *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.
[44] *Id.* Art. 35(1).
[45] *NIST RFI* at 56825.
[46] Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5, *available at* https://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html.
[47] California Consumer Privacy Act of 2018 (A.B. 375), *available at* https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375.
[48] Federal Trade Commission Act, 15 U.S.C. § 45.

privacy requirements, like the CPNI requirements under the Communications Act,[49] the Health Insurance Portability and Accountability Act ("HIPAA"),[50] the Gramm-Leach-Bliley Act ("GLBA"),[51] the Children's Online Privacy Protection Act ("COPPA"),[52] or others. Different risks are addressed under these different regimes.

D. NIST should not rely too heavily on its work on federal government privacy because there are key distinctions between federal and non-federal organizations.

There are key differences between federal and non-federal organizations. For example, non-federal organizations tend to have greater diversity than federal organizations, with vastly different organizational structures, hierarchies, reporting obligations, sizes, customer bases, missions, etc. While there is diversity across the federal government, the range is not as great. For example, different federal organizations have varying missions; however, they often have commonalities that cannot be found across the private sector, including reliance on federal funds. Federal organizations also collect, maintain, use, and share information differently than non-federal organizations. Federal organizations and non-federal organizations deal with different types of data. Indeed, federal systems can handle highly sensitive data, data that citizens and others are required to provide to the government, classified information, and critical national security data, among others.

Not surprisingly, federal organizations are subject to different legal frameworks than typical private organizations. In the case of privacy, federal agencies must comply with the

[49] *See* 47 U.S.C. § 222; 47 C.F.R. §§ 64.2001 *et seq.*
[50] Health Insurance Portability and Accountability Act of 1996, P.L. 104-191, 110 Stat. 1936 (1996).
[51] *See* 15 U.S.C. § 6802.
[52] *See* 15 U.S.C. § 6501-6505.

Privacy Act of 1974,[53] OMB policies including OMB Circular A-130,[54] and Federal Information Processing Standards.[55] Non-federal organizations, on the other hand, operate under various regimes.

Given these differences, importing NIST's work on privacy, which has been largely in the context of federal organizations, would be unhelpful. It would undermine NIST's effort to develop a Privacy Framework that is compatible with varied privacy approaches. For example, NIST's privacy work in the context of federal systems—NISTIR 8062—is an informative work product; however, it is tailored to the federal government's collection and use of data. To the extent NIST relies on or highlights NISTIR 8062 in the Privacy Framework, it should do so only as an informative reference and with a clear explanation of its federal government focus.

IV. NIST'S PRIVACY FRAMEWORK SHOULD BE GENERAL ENOUGH TO BE USED BY ORGANIZATIONS OF VARYING PRIVACY POSTURES.

A. The Privacy Framework should be a starting point for organizations to assess and improve their management of privacy risk, not an end state.

Different organizations will use the Privacy Framework differently. It should be able to aid organizations where privacy has not typically been a top concern, as well as organizations with robust privacy programs. For organizations with limited resources to devote to privacy or that have not previously considered risks because they are not directly regulated or possess relatively little consumer data, the Privacy Framework will be critical, because it can help them think about how to approach organizational privacy challenges and ask questions that can serve as a baseline. CTIA is optimistic that the Privacy Framework can be like the Cybersecurity

[53] 5 U.S.C. § 552a.
[54] Office of Mgmt. & Budget, Exec. Office of the President, Circular No. A-130, *Managing Information as a Strategic Resourc*e (July 28, 2016), https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf.
[55] NIST, Current Federal Information Processing Standards, https://www.nist.gov/itl/current-fips (last visited Dec. 19, 2018).

Framework and complement or validate mature programs in organizations where risk management principles are built into day-to-day operations—like many in the wireless sector.

Given the lack of generally applicable privacy baselines, NIST's work can be very helpful as a starting point for the private sector. In the future, NIST can ask stakeholders how a Privacy Framework can help organizations iterate on mature programs, such as considering third-party privacy. This might include, for example, understanding privacy policies and the practices of external organizations, like those with which an organization might merge or want to acquire. Such topics would be appropriate for inclusion in a Roadmap accompanying the Privacy Framework.

B. The Privacy Framework should offer general, value-agnostic guidance for organizations to flexibly apply.

As explained above, the Privacy Framework should not establish privacy policy terms or substantive expectations, or make value judgments for organizations. Doing so would undermine NIST's commitment to developing a "risk-based, outcome-based, voluntary, and non-prescriptive" framework.[56]

NIST can identify threshold questions that will help organizations assess their privacy posture without suggesting what any organization's posture should be. For example, an organization may be encouraged to ask itself:

- What stakeholders are relevant? (Employees, customers, third parties whose data your organization touches, but with whom the organization does not have a direct relationship?)
- Where are the stakeholders located?
- What types of data does your organization collect, maintain, or store?
- What services does your organization offer and to whom?

[56] *NIST RFI* at 56825.

- Does your organization share data with third-parties, including service providers and vendors?
- What privacy regulations or requirements are applicable to your organization?

Assessing privacy posture is an important first step for an organization to understand its needs and potential risks and challenges, providing the foundation for developing risk- and outcome-based privacy programs.

The Privacy Framework might also include questions highlighting key elements of a robust privacy program. The Privacy Framework should not reflect value judgments about possible answers. Questions might include:

- Does your organization have procedures for mapping data flows, including how your organization collects, uses, manages, and shares information?
- Does your organization have internal privacy policies that address issues such as data collection, data classification, use and sharing practices, data security, and internal processes?
- Does your organization have customer-facing privacy policies?
- Does your organization have controls and policies for managing the sharing of personal data with third parties, including vendor management and APIs.
- Does your organization have an oversight and compliance program to monitor adherence to established privacy policies and processes?
- Is there a person or office in your organization that coordinates oversight and compliance programs?
- Does your organization impose consequences for failure to adhere to established privacy policies and processes?
- Does your organization have a privacy training program?
- Is there a person or office in your organization that is responsible for privacy training programs?
- Does your organization incorporate Privacy by Design practices that, where appropriate, encourage the development of systems that collect and store personal data?

- Does your organization conduct privacy impact assessments for higher-impact use cases? Considerations may include customer expectations (e.g., customer-facing privacy policies and choices), technical issues such as de-identification, and legal and regulatory requirements.

- Does your organization have a data security program, as addressed in the Cybersecurity Framework?

- Does your organization have documented procedures for individuals to report privacy issues?

- Does your organization have an established a data breach response plan?

Through these questions, NIST could encourage organizations to explore effective privacy practices. This in turn would promote voluntary adoption of risk-based approaches to manage privacy risks within organizations.

V. CONCLUSION

CTIA looks forward to working with NIST and other stakeholders to collaborate on a voluntary, flexible, and policy neutral framework for assessing and improving privacy practices. By engaging with stakeholders early and often, NIST has the opportunity to develop a Privacy Framework that meaningfully facilitates innovative and beneficial uses of data while encouraging adoption of risk-based safeguards to improve consumer privacy. CTIA is pleased to participate in this important effort.

Respectfully submitted,

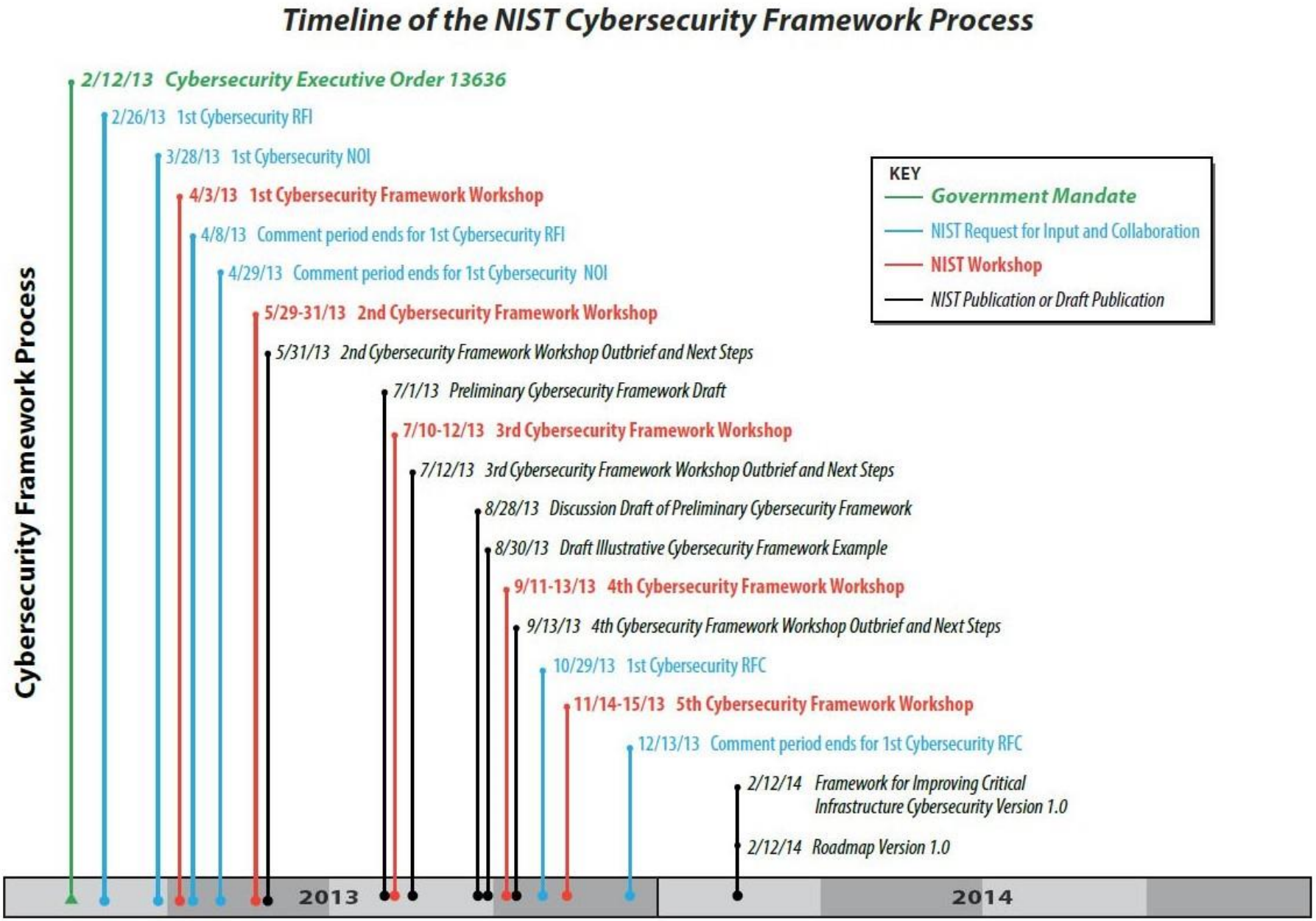
Melanie K. Tiano
Director, Cybersecurity and Privacy

Thomas C. Power
Senior Vice President and General Counsel

CTIA

www.ctia.org

Appendix


Timeline of the NIST Cybersecurity Framework Process
Cybersecurity Framework Process
2/12/13 Cybersecurity Executive Order 13636
2/26/13 1st Cybersecurity RFI
3/28/13 1st Cybersecurity NOI
4/3/13 1st Cybersecurity Framework Workshop
4/8/13 Comment period ends for 1st Cybersecurity RFI
4/29/13 Comment period ends for 1st Cybersecurity NOI
5/29-31/13 2nd Cybersecurity Framework Workshop
5/31/13 2nd Cybersecurity Framework Workshop Outbrief and Next Steps
7/1/13 Preliminary Cybersecurity Framework Draft
7/10-12/13 3rd Cybersecurity Framework Workshop
7/12/13 3rd Cybersecurity Framework Workshop Outbrief and Next Steps
8/28/13 Discussion Draft of Preliminary Cybersecurity Framework
8/30/13 Draft Illustrative Cybersecurity Framework Example
9/11-13/13 4th Cybersecurity Framework Workshop
9/13/13 4th Cybersecurity Framework Workshop Outbrief and Next Steps
10/29/13 1st Cybersecurity RFC
11/14-15/13 5th Cybersecurity Framework Workshop
12/13/13 Comment period ends for 1st Cybersecurity RFC
2/12/14 Framework for Improving Critical Infrastructure Cybersecurity Version 1.0
2/12/14 Roadmap Version 1.0
2013
2014
KEY
Government Mandate
NIST Request for Input and Collaboration
NIST Workshop
NIST Publication or Draft Publication