January 14, 2019

Katie McFarland
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

Via e-mail to: privacyframework@nist.gov

RE: ITI comments in response to NIST RFI - "Developing a Privacy Framework" [Docket Number 181101997-8997-01]

Dear Ms. McFarland:

The Information Technology Industry Council (ITI) appreciates the opportunity to respond to the Request for Information (RFI) noticed by the National Institute of Standards and Technology (NIST) on November 14, 2018, "Developing a Privacy Framework."

ITI is the global voice of the tech sector. We are the premier advocate and thought leader in the United States and around the world for the information and communications technology (ICT) industry. ITI's members comprise leading technology and innovation companies from all corners of the ICT sector, including hardware, software, digital services, semiconductor, network equipment, internet companies, and companies using technology to fundamentally evolve their businesses.

Privacy is a longstanding ITI policy priority, as protecting privacy is integral to our members' businesses and establishing and maintaining consumer trust. Consumer trust is a key pillar of innovation, and our industry must do everything it can to deepen that trust and meet our customers' expectations when it comes to protecting their privacy and personal data. NIST's RFI is an important step toward developing a Privacy Framework that can serve as a tool to help organizations better manage privacy risks while fostering customer trust in products and services in an increasingly connected and complex technology environment - powered by innovations including artificial intelligence and the Internet of Things - and a global policy environment marked by rapidly evolving laws and regulations.

ITI responds to this RFI from the perspective of ITI as a trade association. We have not answered all 26 questions individually, but rather have responded to each of the three question sets, indicating answers to specific enumerated questions (referenced in **bold**) as appropriate. In addition, immediately below we offer some summary comments and general observations.

Summary Observations: NIST's Privacy Framework Approach

We applaud the Department of Commerce's forward-thinking approach to addressing modern privacy challenges, as expressed in both the National Telecommunications and Information Administration's (NTIA) recent RFC on developing the administration's approach to consumer privacy and NIST's RFI to inform development of a privacy risk management framework. These complementary efforts can play a critical role in informing the development of federal privacy legislation in the U.S., and in providing companies and other organizations with robust tools to meaningfully implement privacy laws at the U.S. federal or state levels, or internationally.

NIST's proposed Privacy Framework can help make ITI's *FAIR on Privacy* actionable. In an effort to better inform the ongoing public discussion regarding privacy, ITI and its member companies developed during the second half of last year a document entitled "Framework to Advance Interoperable Rules (FAIR) on Privacy" *(FAIR on Privacy*), a roadmap for legislation to protect privacy and personal data to advance the interests of all stakeholders, including individuals, businesses, and governments. We anticipate this work will continue to take shape as we work alongside consumer advocates, lawmakers, industry partners, and other key stakeholders in the administration, including NIST and NTIA, and beyond to advance meaningful federal privacy legislation in the United States.

FAIR on Privacy sets forth specific ideas that advance the privacy rights of individuals and makes explicit the responsibilities of companies in using personal data while continuing to deliver the innovative products and services consumers and businesses demand. As NIST notes in the RFI, it can sometimes be a "challenge to design, operate, or use technologies in ways that are mindful of diverse privacy needs in an increasingly connected and complex environment," and we welcome the opportunity to work with NIST and other stakeholders through the Privacy Framework development process to help provide tangible implementation guidance that helps companies put in action the concepts discussed in *FAIR on Privacy*. Adoption of elements of *FAIR on Privacy* will give consumers more control and a clearer understanding of their choices regarding the use of their personal data. It also clearly defines an entity's responsibilities so they can be held accountable by regulators, thereby ensuring companies use personal data responsibly and transparently.

A Privacy Framework is useful whether or not U.S. federal privacy legislation is ultimately enacted, as companies will be well-served by a Privacy Framework that offers voluntary guidance on how to implement the principles we advocate any privacy legislation should contain, including how to responsibly and transparently use personal data, increase consumer control, establish accountability and responsibility, promote security, and otherwise manage privacy risks. Even absent U.S. federal privacy legislation, the Privacy Framework envisioned by NIST may nonetheless prove valuable for companies seeking to

implement existing or future privacy requirements (wherever their origin), or to simply serve as a tool for organizations seeking to improve their management of privacy risks.

NIST's Cybersecurity Framework is a laudable model for the Privacy Framework. We commend NIST for its leadership in developing a Privacy Framework intended to help organizations better identify, assess, manage, and communicate privacy risks. NIST has a long history of leadership in furthering sound risk management approaches, including NIST's development of the voluntary *Framework for Improving Critical Infrastructure Cybersecurity* (the "Cybersecurity Framework"), which ITI has supported and contributed to since its inception. As further elaborated below, we believe it is important to develop the Privacy Framework in a way that is aligned with and complementary to the Cybersecurity Framework from the outset. The Cybersecurity Framework leverages public-private partnerships, is grounded in sound risk management principles, and helps foster innovation due to its flexibility and basis in global standards. It embodies an approach well-worth emulating as NIST's Privacy Framework effort takes flight.

NIST's proposed Privacy Framework attributes largely hit the mark. NIST proposes seven minimum attributes the Privacy Framework should possess in order to be effective. We agree all seven of the attributes NIST identifies are necessary. Herein we propose clarifications for some of the attributes, particularly to highlight the need for the Privacy Framework to prioritize flexible and nimble risk management-based solutions, and to leverage or foster the development of global standards and best practices to drive international alignment and harmonization.

Developing a Privacy Framework Roadmap in conjunction with the Privacy Framework is essential. Just as NIST published a Roadmap in conjunction with the Cybersecurity Framework, NIST should plan to publish a Roadmap in conjunction with the Privacy Framework that highlights key areas where additional work to develop and build consensus around privacy standards and best practices is necessary. Indeed, a more robust Roadmap will likely be necessary to map Privacy Framework development areas given the relative dearth of well-established consensus privacy risk management standards and best practices, as compared to the significant number of established cybersecurity standards available when the Cybersecurity Framework was created.

Question Set 1: Organizational Considerations

As we survey the global landscape, **one of the greatest challenges (Q.1)** we find is the frequent lack of clarity in privacy laws or regulations, or, alternatively, that such requirements are overly prescriptive and burdensome, draining resources from other legitimate and potentially more effective privacy protection methods. As a result, regulatory regimes in multiple geographic or sectoral domains are often simply difficult to

implement, particularly for small- and medium-sized enterprises (SMEs). Additionally, many organizations operating globally are subject to regulatory regimes with overlapping audit requirements – sometimes with contradictory privacy risk criteria – creating difficult and burdensome global compliance challenges for companies of all sizes.

The Privacy Framework will prove valuable if it can serve as a common and accessible language for managing privacy risks, as creating a global lexicon containing clearly defined parameters of identifying, assessing, managing, and communicating privacy risk would go a long in way in easing compliance challenges created by prescriptive, overlapping, conflicting and/or fragmented requirements.

We agree that all seven of the **core minimum attributes NIST identifies in the RFI are necessary to make the Privacy Framework effective (Q. 8)**:

1. *Consensus-driven and developed and updated through an open, transparent process.*
2. *Common and accessible language.*
3. *Adaptable to many different organizations, technologies, lifecycle phases, sectors, and uses.*
4. *Risk-based, outcome-based, voluntary, and non-prescriptive.*
5. *Readily usable as part of any enterprise's broader risk management strategy and processes.*
6. *Compatible with or may be paired with other privacy approaches.*
7. *A living document.*

We suggest further fleshing out the description accompanying #3 in the RFI, *adaptable to many different organizations, technologies, lifecycle phases, sectors, and uses,* in a few respects. First, to add **dynamic privacy risks** as one of the reasons we need an adaptable Privacy Framework. Second, to clarify that **flexible and nimble risk management solutions** are called for to ensure the Privacy Framework is adaptable to address the various components spelled out in the attribute. And third, to clarify that the concept of "platform- and technology-agnostic and customizable" translates into a Privacy Framework that is not only technology-neutral but **does not prescribe or mandate the use or deployment** of technologies, technical solutions or tools.

We also suggest expanding the description accompanying #6 in the RFI, *compatible with or may be paired with other privacy approaches*, to emphasize **the importance of promoting global, voluntary, consensus-based standards and best practices**, to better leverage industry's efforts and resource commitments and to reflect the borderless nature of cyberspace. Global ICT standards respond broadly to the needs of global markets, demonstrate relevance through voluntary worldwide adoption and implementation, and are products of standardization processes that are consensus-based, transparent, and

industry-led with participation open to any interested party. Additionally, the description accompanying attribute #6 could better articulate the need to leverage existing global privacy standards and best practices (where available) and stress the importance of further global standards development to drive international alignment and harmonization, and to promote development of a Privacy Framework that can gain traction globally.

We believe that an **outcome-based approach to privacy (Q. 9)** should look very much like the approach identified in NTIA's RFC, which expressly articulates the core privacy outcomes that consumers should expect from organizations and the high-level goals for federal action – transparency, control, reasonable minimization, security, access and correction, risk management, and accountability. We support the key outcomes and end goals identified by NTIA, which are aligned with the key outcomes and goals we believe form a key part of any meaningful privacy framework as set forth in our *FAIR on Privacy*. We further elaborate on four key outcomes articulated in *FAIR on Privacy* below.

Enhance Transparency. *FAIR on Privacy* recommends that individuals should be informed of the collection and use of their personal data in a way that is meaningful, clear, obvious, and useful so they have a better understanding of what they are (or are not) consenting to with respect to their personal data. This includes being informed of the categories of companies (including third parties) who collect their personal data and how they use it. We believe our expression of this outcome in *FAIR on Privacy* builds on the position outlined by NTIA in its RFC but further elaborates the specific commitments that companies should be required to make to enhance transparency and create "informed consumers." NIST's Privacy Framework can play an important role in identifying, organizing, and communicating privacy risk management standards and best practices to help organizations implement enhanced transparency.

Increase Consumer Control. We agree with NTIA that one of the chief goals of a privacy framework should be to give users control of their personal information while also avoiding process-heavy approaches that challenge the equal and vibrant participation of SMEs. The best way to achieve this is through a model that balances the various interests while being uncompromising in the protection afforded to individuals. *FAIR on Privacy* recognizes that individuals should have the right to expressly and affirmatively consent to the use of their sensitive personal data, and to be able to access, correct, port, delete, and object to the use of their personal data where it is appropriate to the context of an organization's business relationship with consumers, and their use of such personal data. Identifying, organizing, and communicating standards and best practices to help organizations implement the many vectors of consumer control is an area ripe for progress via NIST's Privacy Framework. Identifying (or identifying for Roadmap development) standards that operationalize the concept of context in data collection and use, to account for how users'

expectations change based on the context in which they utilize technology, and how companies interact with users, would be a welcome focus area for the Privacy Framework.

Establish Company Responsibility and Accountability. *FAIR on Privacy* fleshes out in detail the responsibilities organizations should have when using personal data, a key question identified by NIST in the RFI (as well as NTIA in its RFC). As articulated in *FAIR on Privacy*, companies should be required to identify, monitor, and document uses of known personal data, and ensure all uses are responsible and permissible under law. Companies transferring personal data to a third party that acts as service provider are further required to perform due diligence to ensure the third party protects such data in accordance with the law and the companies' commitments to their customers. This includes ensuring that the third party employs appropriate controls, contractually binding the third party to assist in upholding the companies' legal responsibilities and requiring the third party to notify the company if it can no longer meet such obligations. We are aligned with NTIA in its RFC that accountability and responsible use are key outcomes of a meaningful privacy framework and have fleshed these concepts out accordingly in *FAIR on Privacy*. Accountability is another area where the Privacy Framework can help organizations that want to embrace accountability concepts such as Privacy by Design. Making progress on identifying, organizing, and communicating standards and best practices in this area can meaningfully assist organizations in implementing privacy by design across their products and services offerings.

Promote Security and Manage Risk. There can be no privacy without security. We appreciate NTIA highlighting in its RFC the importance of security as a key outcome to ensure a privacy framework is effective, and of course NIST is aware of the "strong nexus" between cybersecurity and privacy, acknowledging in Cybersecurity Framework Ver. 1.1 that "it is well recognized that cybersecurity plays an important role in protecting privacy." *FAIR on Privacy* explicitly recommends that companies be required to implement comprehensive security programs that can support and protect a company's operations, activities, and information. Similar to what NTIA has alluded to in its RFC, our framework recommends that companies comprehensively identify, assess, and monitor the privacy risks to individuals relating to the use of personal data, take reasonable steps to mitigate these risks, and balance the possible benefits of personal data use to individuals, other stakeholders, and society at large. As NIST builds the Privacy Framework, there is clearly an opportunity to do so in a way that prioritizes the key outcome of security, including by creating a Framework structure that makes it easy to identify touchpoints to relevant data protection and other relevant standards contained within the Cybersecurity Framework.

Aside from our *FAIR on Privacy* principles, **several standards, frameworks, models, methodologies, tools, guidelines, and best practices already exist and help organizations in identifying, assessing, managing, and communicating privacy risk at the management,**

operational and technical levels (Q. 10). For example, the *EU-U.S. Privacy Shield Framework* (*Privacy Shield*) program administered by the Department of Commerce imparts heightened responsibilities on certified companies to manage various aspects of their privacy risks when transferring personal data out of the EU to companies in the U.S. While the text of the *Privacy Shield* does not explicitly call for an audit or assessment of third-party vendors, the Federal Trade Commission (FTC) serves as the *Privacy Shield* enforcement authority and has traditionally required some form of due diligence by the company of the third party to ensure that contract language is adequately enforced.

The *Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) system* is another model. The APEC CBPR is a voluntary but enforceable certification program designed to ensure the continued free flow of personal information across APEC member economy borders, while establishing meaningful protection for the privacy and security of personal information. In order to obtain an APEC CBPR certification, companies must vet their privacy policies and requirements against numerous CBPR program requirements covering data collection, use, security, access and correction, as well as company accountability and a host of other requirements.

The *EU's Binding Corporate Rules* (BCRs) similarly serve as a like a code of conduct in that they allow multinational companies to transfer personal data across borders and outside of the EU while ensuring that all data transfers within the corporate group are sufficiently protective of individual privacy. BCRs contain privacy principles, tools of effectiveness, and an element proving that the rules are binding.

Additionally, many stakeholders now consider the EU's *General Data Protection Regulation (GDPR)*, which came into force in May 2018, a de facto global privacy standard. Due to its extraterritorial scope and provisions on cross-border data transfers, GDPR is having a global impact, inspiring other countries considering updating their privacy regimes to align with the GDPR. The risk management and data protection impact assessment approaches laid out therein have also become influential for many companies who have imposed GDPR-compliant internal processes across their global operations. Some organizations find the regulatory requirements of GDPR and other regimes difficult to implement, due to a lack of existing clear implementation guidance and other issues – the contemplated NIST Privacy Framework could prove helpful in filling this gap.

There are also several noteworthy industry-led efforts. For example, the *Network Advertising Initiative (NAI) 2018 Code of Conduct* (the "Code") consolidates requirements for web-based and app-based data collection and use into one document, incorporating previous NAI Guidance documents and updating terminology. The Code imposes notice, choice, accountability, data security, and use limitation requirements and incorporates a rigorous compliance and enforcement program that includes annual reviews, ongoing technical monitoring, investigation of complaints, and enforcement procedures.

Internet Advertising Bureau (IAB) Europe's Transparency & Consent Framework (the "IAB Europe Framework") is another good resource that helps parties in the digital advertising chain understand how to comply with the requirements of the GDPR and ePrivacy Directive[1] when processing personal data or accessing and/or storing information on a user's device, such as cookies, advertising identifiers, device identifiers, and other tracking technologies.

The IAB Europe Framework is particularly relevant for first-parties, such as publishers and other suppliers of online services, who work with third-parties for data-driven services, such as digital advertisers and other partners. Using the IAB Framework, first-parties can enable third-parties to process user data on one of the legal bases of EU regulation. The IAB Europe Framework standardizes the presentation to users' third-party data processing requests that require "informed" consent for data processing. The IAB Europe Framework enables "signaling" of user choice across the advertising supply chain. It is open-source and not-for-profit with consensus-based industry governance led by IAB Europe with significant support from industry players.

Importantly, NIST should approach the Privacy Framework as a tool for organizing and synthesizing the above-listed and other standards, frameworks, models, methodologies, tools, guidelines, best practices, and principles that organizations are using to identify, assess, manage, and communicate privacy risk at the management, operational, and technical levels. Listed above are just some of the examples that ITI and its members are aware of; we expect additional examples will be identified by other filers and in subsequent Privacy Framework workshops. To the extent gaps are identified that are not adequately covered by existing standards, frameworks, models, methodologies, tools, guidelines, best practices, and principles, NIST should seek to address these standards as development areas in the Roadmap, rather than in the Privacy Framework proper.

Current regulatory or regulatory reporting requirements in the U.S. and internationally have had an inconsistent relation to the use of standards, frameworks, models, methodologies, tools, guidelines and best practices, and principles (Q. 11). The United States has a history of voluntary adoption of robust privacy protections and rigorous enforcement under the oversight of the FTC. This has given rise to the development of innovative and best in class privacy enhancing techniques like anonymization, encryption, and security risk management and is an example of the virtue of a flexible, single regulatory approach implemented at the federal level.

[1] The EU's 2002 *ePrivacy Directive* establishes rules regarding the confidentiality of communications, as well as tracking and monitoring. https://edps.europa.eu/data-protection/our-work/subjects/eprivacy-directive_en

Contrary to this example is the patchwork of data breach notification regimes below the U.S. federal level. There are currently 54 state and territory laws governing notification to consumers in the wake of an unlawful breach of data security. Across those 54 schemes, there is variance – sometimes contradictory – in the "risk trigger" (indicating when a notification must be made), the definition of "personal data," and in the timeframe for notification, leading to inconsistent notices for consumers depending on where they reside. This check-the-box-in-54-different-ways approach unnecessarily slows down consumer notification because of the time it takes to cross-verify compliance with 54 regimes versus cross-verifying with one law.

On the international level, there is a growing focus on the use of standards, models, or frameworks to demonstrate compliance with privacy principles and laws. Many countries are in the process of instituting audit requirements on the handling of personal data in line with their own domestic laws/standards as further explained in the paragraphs below.

Several countries are currently considering **mandates to use specific standards, frameworks, models, methodologies, tools, guidelines and best practices, and principles in ways that create potential conflicts between requirements and desired practices (Q. 12).** China provides a prime example, as its Cyber Security Protection Bureau issued a draft *Guideline for Internet Personal Information Security Protection* along with a request for public comments on November 30th, 2018. Even though the guideline will not be mandatory, it nonetheless plays a key implementing role in relation to *China's Cyber Security Law* and related recent measures governing the protection of information systems and personal information in China. A company subject to China's rules may face supervision from several different authorities who could potentially enact their own overlapping or conflicting rules, calling into question the voluntary nature of the guidelines.

India's *Srikrishna Expert Committee on Data Protection* released a draft *Report and Data Protection Bill* that would require maintaining the records of data processing and impact assessments. It also introduces the concept of an annual data audit conducted by independent data auditors to ensure companies' compliance with the requirements in the proposed bill.

The EU's GDPR does not mandate the use of certifications but suggests their use as a way of demonstrating that the processing of personal data complies with GDPR requirements. The GDPR states that certification is also a means to demonstrate compliance with the provisions on data protection by design and by default (Article 25(3)); demonstrate that an organization has appropriate technical and organizational measures to ensure data security (Article 32 (3)); and to support transfers of personal data to third countries or international organizations (Article 46(2)(f)). EU member states, supervisory authorities, the European Data Protection Board (EDPB), and the EU Commission plan to promote certification as a mechanism to enhance transparency and compliance with the GDPR.

In the examples above, government organizations and bodies around the world are beginning to develop national standards and tools for assessing and managing privacy risk. While the focus on developing privacy standards is in many ways a positive development, the fragmented nature of these efforts is a cause for concern. Each of these initiatives primarily remains inward-focused, within a country or region's borders, and divorced from the reality that global companies today operate in multiple jurisdictions and are subject to overlapping – and sometimes contradictory – audit and risk management compliance requirements.

It is essential that **national initiatives, standards, and organizations are coordinated on an international level to promote scalable and mutually interoperable models and best practices (Q.13)** that enable companies to demonstrate their compliance with multiple national privacy obligations through a single, streamlined internal privacy risk management approach**.** The *International Conference of Data Protection and Privacy Commissioners* (ICDPPC) is one possible coordinating platform for countries to share and coordinate their efforts towards developing globally interoperable approaches to privacy risk management. The ICDPPC adopted a resolution during its 40th session in 2018 to strengthen the Conference as a more efficient platform for international cooperation and policy influence, a more diverse, open and transparent network, and a more structured and efficient organization. Additionally, we are hopeful the Privacy Framework could itself serve as a focal point for driving future conversations around global interoperability, by serving as a tool to help companies implement requirements across multiple jurisdictions.

There are several potential positive **international implications of a Privacy Framework on global business or in policymaking in other countries (Q. 14).** ITI's members are global companies with headquarters or offices in various and multiple countries. Most ITI companies service the global market via complex global supply chains in which products are developed, made, and assembled in multiple countries across the world. As a result, we acutely understand the impact of international policies on innovation and the need for governments' policies to be globally compatible. Privacy approaches that differ dramatically by country — a policy patchwork — not only create potentially negative consequences for privacy and consumers but also disrupt global commerce and ignore the borderless nature of the Internet.

We hope this Privacy Framework leads to greater global consensus for privacy policymaking and sends a signal to our digital trading partners about the importance of and the most effective ways to implement privacy risk management practices. To achieve a global consensus, it would be helpful if the United States solicits comments and support from other countries during development of the Privacy Framework. Further, it is important that the U.S. Government set a positive example regarding the essential role that global standards play for both industry and government. NIST should establish a

preference that any consensus-based standards referenced the Privacy Framework also be *global* to reflect the realities of cyberspace and the ICT marketplace, better facilitate global deployment of privacy protection measures, and help reduce barriers to trade.

Similar to the Cybersecurity Framework, this Privacy Framework will potentially – and ideally – be emulated by other governments around the world in their policy environments and be embraced by businesses operating globally as a tool for implementing international privacy requirements. We will advocate for and strongly support such efforts because they would create consistent and cohesive approaches across geographies as well as a commitment to the global standardization process, public-private partnerships, and a voluntary—as opposed to regulatory--approach. Thus, NIST has a strong incentive to make sure any Privacy Framework developed would be equally beneficial if deployed globally.

Question Set 2: Structuring the Privacy Framework

How NIST structures and organizes the Privacy Framework is a key threshold issue for a variety of reasons, including (1) communicating privacy risk assessment and management to multiple stakeholders within companies (e.g., executives to privacy engineers); (2) effectively creating a common language across sectors, organizations of multiple sizes, technologies and use cases; and (3) ensuring alignment with the Cybersecurity Framework in a complementary (but not redundant) fashion.

Numerous aspects of the Cybersecurity Framework could serve as a model for the Privacy Framework, and we encourage NIST to be mindful of the relationship between the two frameworks throughout the Privacy Framework development process (Q. 17). We commend NIST for its leadership in undertaking to develop a Privacy Framework intended to help organizations better identify, assess, manage, and communicate privacy risks. NIST has a long history of leadership in furthering sound risk management approaches, including NIST's work in developing the Cybersecurity Framework, which ITI has supported and contributed to since its inception. We believe it is important to develop the Privacy Framework in way that is aligned with and complementary to the Cybersecurity Framework from the outset. The Cybersecurity Framework leverages public-private partnerships, is grounded in sound risk management principles, and fosters innovation due to its flexibility and basis in global standards, thus is worth emulating here.

Further, many organizations are currently utilizing the Cybersecurity Framework, and one of the key questions on the mind of many is how these stakeholders will be able to use the Privacy Framework in concert with the Cybersecurity Framework. As NIST is aware, the Cybersecurity Framework makes clear as part of its **core methodology** that organizations using the Cybersecurity Framework should consider the potential impacts of their cybersecurity activities on individual privacy and civil liberties throughout their cybersecurity risk management practices, and the Cybersecurity Framework catalogues

many data protection and other privacy-relevant standards in the Informative References. ITI companies are committed to ensuring their customer information is afforded appropriate privacy protections and ITI supports the Cybersecurity Framework's approach of treating privacy and security in an integrated fashion, which mirrors the approach of those companies who integrate their security and privacy risk-management functions and practices.

Pursuing a structure similar to the Cybersecurity Framework is appealing in many respects and should receive serious consideration, particularly if comments to the RFI validate there is broad stakeholder consensus to align the Privacy Framework and Cybersecurity Framework. Emulating the Cybersecurity Framework's hierarchical structure of core functions, categories, subcategories, and informative references seems a straightforward way to help drive that result, as doing so would provide stakeholders with a recognizable format, familiar risk management terminology, and would provide a common lexicon or taxonomy that would accelerate the Privacy Framework's utility as a communications tool. The Cybersecurity Framework's **profiles** concept would also be welcome in the context of a Privacy Framework – every organization need not try to achieve every possible privacy outcome, but rather should have the latitude to tailor privacy risk management solutions depending on a given organization's profile, including factors such as the company's size, technology products and services, and relationship to its customers, as well as the varying contexts in which consumers interact with technologies and services, and in which companies interact with or use consumers' data.

The Cybersecurity Framework is a living monument to the concept that "one size doesn't fit all"– this is as true in the privacy risk management context as it is in the cybersecurity risk management context, and whatever Privacy Framework NIST develops should reflect this fact.

For all these reasons, it is essential that the Privacy Framework be constructed with an eye toward the existing Cybersecurity Framework, in terms of both structure and substantive approach.

While each of the **organizing constructs for the Privacy Framework identified by NIST in Q. 18** doubtless has merit, for the reasons stated immediately above, NIST should prioritize **pursuing a structure and construct similar to the Cybersecurity Framework**, while perhaps integrating concepts or terminology from some of the other constructs within this structure as appropriate.

For example, **principles such as the FIPPs** continue to have enduring vitality in a variety of contexts, including informing ITI's FAIR on Privacy, NTIA's contemplated privacy framework, and various other sets of principles and legislative efforts globally. The FIPPs also provide familiar terminology to many stakeholders, so incorporating references to the

FIPPS may facilitate achieving a Privacy Framework that can serve as a common language accessible to multiple stakeholders across multiple technologies, use cases, and contexts.

Question Set 3: Specific Privacy Practices

While ITI has anecdotal evidence that many of the **core privacy practices identified in question set three (Qs 19-26)** are in widespread use across the tech sector and beyond, we do not possess enough information to speculate on the "degree of adoption" of such practices. We look forward to further discussions on this topic, including whether any other core privacy practices exist that merit inclusion in the Privacy Framework, during the workshops.

Conclusion

We thank NIST for its commitment to partnering with the private sector to advance our shared privacy goals. We also commend NTIA, the Department of Commerce, and the Administration more broadly for its willingness to engage with our companies and the ICT industry generally to determine how government and industry can best work together to improve privacy protections. The commitment to stakeholder outreach is an excellent example of how public-private partnership processes, which have proven so effective in improving cybersecurity, can also help advance privacy.

ITI and its members look forward to continuing to work with NIST to develop the Privacy Framework, and on other initiatives to improve privacy protections while maintaining innovation and ensuring trust. Please continue to consider ITI a resource on privacy issues moving forward and do not hesitate to contact us with any questions regarding this submission.

Sincerely,

John Miller
Vice President, Policy and Law