From: Courtney Lang <clang@itic.org>
Sent: Thursday, October 24, 2019 1:35 PM
To: privacyframework <privacyframework@nist.gov>
Cc: Lefkovitz, Naomi B. (Fed) <naomi.lefkovitz@nist.gov>; Sedgewick, Adam (Fed) <adam.sedgewick@nist.gov>; Nadeau, Ellen M. (Fed) <ellen.nadeau@nist.gov>; Boeckl, Kaitlin R. (Fed) <kaitlin.boeckl@nist.gov>; John Miller <JMiller@itic.org>; Alexa Lee <ALee@itic.org>
Subject: ITI Comments on Preliminary Draft of NIST Privacy Framework

Dear Ms. McFarland,

Please find attached the Information Technology Industry Council's (ITI) comments on the Preliminary Draft of NIST's Privacy Framework. We appreciate the opportunity to provide feedback and would be happy to discuss our perspectives further.

Best,

Courtney Lang

Director of Policy

Trust, Data, & Technology

Information Technology Industry Council (ITI)

w: +1 (202) 897-4525

clang@itic.org

ITI Promoting Innovation Worldwide

October 24, 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 on Preliminary Draft of NIST's Privacy Framework:

Dear Ms. McFarland,

The Information Technology Industry Council (ITI), appreciates the opportunity to submit the following comments on the *Preliminary Draft of the NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management* ("Privacy Framework") developed by the National Institute of Standards and Technology (NIST).

ITI is the premier advocate and thought leader in the United States and around the world for the information and communications technology (ICT) industry, and represents leading companies from across the ICT sector, including hardware, software, digital services, semiconductor, network equipment, cybersecurity and Internet companies. 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.

We applaud NIST's efforts in building the Privacy Framework as a tool for organizations seeking to improve privacy risk management. The Privacy Framework additionally can provide valuable guidance to organizations seeking to comply with an evolving landscape of privacy laws and regulations globally and the United States. We are also grateful that the Preliminary Draft reflects many of the comments we offered in response to NIST's initial November 2018 RFI on the Privacy Framework.[1] In particular, we strongly support NIST's efforts at aligning the structure of the Privacy Framework to that of the successful Cybersecurity Framework. That the Privacy Framework shares a similar structure (Core, Profiles, Implementation Tiers) with the Cybersecurity Framework will help organizations utilize both tools to mitigate privacy risks, including in those areas of overlapping cyber and privacy risks, such as in the data breach context.

[1] ITI's Comments in response to NIST RFI: "Developing a Privacy Framework." January 14, 2019. Available at: https://www.nist.gov/sites/default/files/documents/2019/02/04/iti_john_miller_508.pdf

Below we offer some additional comments and recommendations regarding the Privacy Framework:

The Target Profiles Help Illustrate the Privacy Framework's Utility as a Flexible Tool. We found the manner in which the Privacy Framework lays out the core, current profile and target profiles, particularly as indicated in *Figure 5: Profile Development Process* (Figure 5), as providing a helpful guide for how companies can use the Privacy Framework to help prioritize their privacy risk management activities and tailor them to their needs, as opposed to as a check-the-box compliance exercise. Figure 5 illustrates the Privacy Framework's flexibility, providing an appropriate overview of an organization's risk management priorities without making it appear as though all aspects of the Privacy Framework core are required for successful mitigation of privacy risk. To provide further clarity, we recommend including in the preamble in Appendix A additional explanation about the importance of users of the Privacy Framework considering the Cybersecurity Framework's Functions, "Detect, Respond, and Recover," in developing their current and target profiles, as a critical component of a privacy risk management system.

The Privacy Framework is Valuable as a Communications Tool. The Privacy Framework demonstrates the potential value of the Privacy Framework as a tool for communicating about privacy, both internally within organizations and externally across their broader privacy ecosystems. Internally, the Privacy Framework can help organizations better understand and more effectively communicate privacy risks across diverse internal stakeholders, including engineering, sales, and legal teams, as well as C-suite executives. Externally, the Privacy Framework can potentially serve as a tool to help organizations communicate how they are managing privacy risks, pointing regulators and other external stakeholders to their privacy practices to and compliance measures.

The Privacy Framework Should Leverage and Reference International Standards. We commend NIST for its leadership in developing the Privacy Framework and modeling numerous aspects of it after the Cybersecurity Framework. However, the lack of references to international standards in the Privacy Framework is notable, particularly as compared to the Cybersecurity Framework. As NIST fleshes out the informative references document published in September along with the Privacy Framework, we recommend adding new and existing international standards such as the ISO/IEC 27701 security techniques[2] – extension to ISO/IEO 27001 and ISO/IEC 27002 for privacy information management. Ultimately, a Privacy Framework leveraging sound risk management principles grounded in global standards will prove the most effective tool for protecting privacy while fostering innovation and economic growth. In addition, many organizations that intend to use the Privacy Framework would benefit from integrating international privacy standards and best practices to further drive global alignment and harmonization.

Develop an Appendix Mapping the Privacy Framework to Privacy Regimes. We appreciate that NIST developed the Privacy Framework as a legislation- and regulation-agnostic tool. However, mapping the Privacy Framework to key international privacy regimes would not only be helpful for

[2] ISO/IEC 27701:2019 Security Techniques. https://www.iso.org/obp/ui/#iso:std:iso-iec:27701:ed-1:v1:en

organizations trying to navigate a complex global regulatory environment, but would help improve the value proposition of the Privacy Framework as a tool that organizations should be using. While in the long term NIST could consider mapping numerous legal regimes to the Privacy Framework, we suggest NIST start by mapping a selection of geographically diverse and internationally impactful regimes, including the European Union's General Data Protection Regulation (GDPR), the Asia Pacific Economic Cooperation (APEC) Cross Border Privacy Rules (CBPR),the EU-US Privacy Shield Framework (Privacy Shield), Japan's Act on the Protection of Personal Information (APPI), Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), and Brazil's new General Data Protection Law. The Privacy Framework holds the potential to provide guidance for organizations who are actively complying with or participating in one or more of these global privacy regimes.

Due to GDPR's extraterritorial scope and impact on cross-border data transfers, GDPR's influence across geographies continues to grow, inspiring other countries to consider updating their privacy regimes to align with the GDPR (such as in the case of Japan's APPI), or to pass comprehensive privacy legislation for the first time (such as Brazil's new law). The GDPR's approaches to risk management and data protection impact assessment have also become influential for many companies who are GDPR-compliant across their global operations. In the Asia-Pacific region, 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. Those companies would benefit from a mapping of the Privacy Framework to the CBPRs, as they could leverage their use of the Privacy Framework to help obtain a CBPR certification. Thousands of companies continue to rely on the Privacy Shield as the key mechanism for enabling transatlantic data flows, and to develop privacy programs and oversight measures that reflect the Privacy Shield Principles. Furthermore, we suggest the Privacy Framework align and map key definitions to the GDPR, and possibly the APEC CBPRs, including the definition of data processing. Given that the control applicability is based on classification of processor or controller, these definitions matter significantly and any discrepancies in definitions can lead to uncertainty and greater potential legal risks for organizations.

Additionally, in the United States, the California Consumer Privacy Act (CCPA), effective in January 2020, is impacting the U.S. federal privacy legislation debate and, once implemented, will potentially set a new privacy standard at the state level. Though the implementation details of the CCPA are still being developed, there are some aspects of the law that might have a potential broader view than the GDPR such as the definition of sensitive data and the protection of minors. Thus, an appendix mapping the key provisions of not only the international regimes referenced above but also the CCPA will help organizations link and make decisions on privacy risk management in the United States and globally.

Consider Adding International Engagement, Small Business Impacts, and Re-Identification Risk to the Roadmap. We support NIST's efforts to develop a Privacy Roadmap in conjunction with the Privacy Framework. Two priority areas we recommend NIST consider adding to the Roadmap are international engagement and alignment and promoting and identifying ways to help small and medium-size enterprises (SMEs) adopt the Privacy Framework. "International Aspects, Impacts, and Alignment" and "Small Business Awareness and Resources" were two areas identified

previously with respect to the Cybersecurity Framework Roadmap, and both should be considered key development areas in the privacy context as well.

International engagement is particularly important given many privacy regimes in the world given little implementing guidance typically accompanies such privacy laws or regulations. When requirements are overly prescriptive or burdensome, the lack of implementing guidance can drain resources from organizations as they seek to comply and divert their attention from potentially more effective privacy risk management activities. The Privacy Framework can serve as an important tool for organizations seeking to consistently manage risks against a panoply of global privacy regulations and requirements.

Additionally, SMEs often have fewer resources to adjust and implement varying regulatory requirements and thus suffer from greater potential exposure to privacy risks. The Privacy Framework will prove valuable if it can serve as a common and accessible language for managing privacy risks, to help mitigate compliance challenges by globally fragmented requirements, especially but not limited to the SMEs.

Finally, given that re-identification risk is currently not considered in the Privacy Framework, ITI recommends including this topic in the Privacy Roadmap and looks forward to partnering with NIST to further develop this area moving forward.

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.

Respectfully submitted,

John Miller, Senior Vice President of Policy and Senior Counsel
Information Technology Industry Council
(202) 499-0034