October 24, 2019

Katie McFarland
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899
privacyframework@nist.gov

Re: NIST Privacy Framework: Preliminary Draft Comments

Dear Ms. McFarland:

The Computing Technology Industry Association (CompTIA),[1] the leading association for the global information technology (IT) industry, respectfully submits these comments in response to the National Institute of Standards and Technology (NIST) request for comments on the draft Privacy Framework.

CompTIA and our member companies have long understood the importance of protecting users' privacy and securing any data that is collected and stored. Although businesses engage in massive efforts to maintain the trust of their consumers by protecting their privacy, governments around the world have also been enacting new privacy and data security laws and regulations. While these laws are often promulgated with the best of intentions, particularly given high-profile data breaches and the pervasive problem of identity theft, the policies contained within these new laws are often more likely to result more in significant compliance costs and stifled innovation rather than improving consumer protection. For example, regulatory regimes such as that recently adopted in California impose one-size-fits-all obligations that create an immense compliance burden for companies without necessarily improving consumer protection.

In contrast, risk-based approaches, such as those proposed by NIST in the draft Privacy Framework, point the way toward a different path. The NIST approach offers a better example for how the United States should make its mark in the consumer privacy and data protection space. Building on NIST's successful Cybersecurity Framework, a risk-based approach to privacy will provide flexibility for companies to meaningfully assess their own operations and protect their users' privacy and the data in their possession in effective ways. The voluntary Privacy Framework would avoid the use of one-size-fits-all checklists or over-reliance on simple notice-and-consent regimes that not only fail to provide adequate privacy protections, but could actually provide a false sense of security, thus undermining privacy. Instead of checking boxes

[1] CompTIA supports policies that enable the information technology industry to thrive in the global marketplace. We work to promote investment and innovation, market access, robust cybersecurity solutions, commonsense privacy policies, streamlined procurement, and a skilled IT workforce. Visit www.comptia.org to learn more.

to ensure compliance with a particular law, the voluntary risk-based framework approach will motivate companies to think more seriously about these issues and implement strong privacy and security practices that best fit their specific business models.

The voluntary NIST Privacy Framework arrives at a time when jurisdictions around the world, including within the United States, are looking to establish their own privacy regulations. The fact that the United States does not yet have a federal privacy law in place has been placing U.S. companies at a disadvantage, and CompTIA has been actively supporting the enactment of a uniform federal privacy law that facilitates a risk-based approach to privacy. While NIST does not (and should not) intend for the voluntary Privacy Framework to be incorporated into law, the Framework nevertheless complements those efforts by demonstrating how such a risk-based approach might work. The success and eventual adoption of the Framework could become an important means to demonstrate how public-private partnerships and risk-based approaches are more effective in ensuring privacy than checklist-style regulation.

Small business. Large U.S. companies are already spending billions of dollars to comply with regulatory mandates on privacy, while some smaller companies are considering cutting off access to their services in areas with overly restrictive privacy laws rather than spending the money necessary to comply. Businesses should not have to choose between compliance and ceasing operations, and the existence of a voluntary Privacy Framework could potentially change the national (and global) dialogue surrounding privacy. For that reason, among others, we urge NIST to give special attention to how the Privacy Framework can be used as a tool by small and medium-sized businesses to meaningfully improve their privacy posture in a manner that is appropriate to the amount and type of data they collect and possess, as well as their risk profile.

We look forward to reviewing the other comments received, and to working with NIST in the future as the Privacy Framework continues to be refined and is eventually made available for use. Thank you for your work on this important project.

Sincerely,

/s/ Dileep Srihari

Dileep Srihari
Vice President & Senior Policy Counsel
CompTIA