Before the
National Institute of Standards and Technology
U.S. Department of Commerce
Washington, D.C. 20230

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

COMMENTS OF USTELECOM

USTelecom – The Broadband Association (USTelecom)[1] is pleased to submit its comments in response to the National Institute of Standards and Technology's ("NIST") Request for Information ("RFI")[2] seeking input on ways to better understand challenges and gaps in privacy practices and gain awareness about how organizations are identifying risk in order to create an enterprise risk and management tool for privacy ("Privacy Framework"). NIST seeks comment on specific topics discussed by stakeholders at its October 16, 2018 workshop so that NIST can develop a roadmap towards a usable and adaptable risk-based, outcome-based and nonprescriptive Privacy Framework[3] in the hope that this tool will ultimately improve organizations' management of processes for incorporating privacy protections into products and services.

---

[1] USTelecom is the premier trade association representing service providers and suppliers for the telecom industry. Its diverse member base ranges from large publicly traded communications corporations to small companies and cooperatives – all providing advanced communications service to both urban and rural markets.

[2] *See Notice Request for Information, NIST, In the Matter of Developing a Privacy Framework*, 83 FR 220, 56824-56827, Docket No. 181101997-8997-01, (Nov. 14, 2018) (*RFI*).

[3] *Id.* at 56825.

USTelecom supports NIST's efforts to work in a collaborative fashion with industry and consumer groups in order to encourage privacy research and voluntary privacy programs and standards that could serve as a safe harbor in legislation, while enabling companies to adapt to rapidly changing technology and market developments. In particular, USTelecom supports the development of a safe harbor that can act as guideposts for companies.

USTelecom views the attributes that NIST identifies for the Privacy Framework (consensus-driven; using accessible language; adaptable to different organizations and technologies; risk-based, outcome-based, voluntary, and non-prescriptive; readily useable as part of an enterprise's broader risk management strategy; compatible with other privacy approaches; and a living document) as well as the discussion topics outlined in the RFI as a good foundation for creating a *voluntary* Privacy Framework. While we agree that NIST should certainly build on its experience developing the successful voluntary Framework for Improving Critical Infrastructure Cybersecurity ("Cybersecurity Framework") in creating its voluntary Privacy Framework, we encourage NIST to defer to other agencies like the Federal Trade Commission (FTC) for policy and regulatory matters. NIST should ensure that its Privacy Framework complements the work of the FTC and the NTIA to develop a policy approach to consumer privacy, so that the result is a harmonized set of guidelines for industry.

We also encourage NIST to avoid a one-size-fits-all approach with respect to privacy and not to mandate a static checklist of requirements. NIST's Cybersecurity Framework has been widely adopted by industry because it is a voluntary, risk-based approach that starts with an overarching framework under which companies have the flexibility to best determine and mitigate their own risks, which will vary by sector, size, and sophistication of individual companies. In that same vein, when considering a Privacy Framework, we encourage NIST to focus on outcomes and avoid establishing an overly rigid or prescriptive framework.

One of the foremost outcomes should be harmonization. For example, in creating the Cybersecurity Framework NIST based its design on widely adopted international standards, furthering a

harmonized approach to cybersecurity. In the same way, NIST should also reference and incorporate established standards and industry guidelines in developing its Privacy Framework so that it is harmonized with current practices that have proven successful where such practices do not conflict with U.S. law or regulatory frameworks. ISO standards and those of the OECD and APEC privacy frameworks should serve as relevant benchmarks. In addition, Privacy Framework should also be technology- and sector-neutral, reflecting that data is collected across multiple services and devices by different types of companies.

For example, as we have noted in other comments,[4] USTelecom sees the FTC privacy framework as the proven method for managing risk based on the sensitivity of the data at issue. The FTC's focus on the net welfare of consumers has successfully balanced both the consumers need for control and access with risks that may be present in the collection and use of data. With that in mind, key elements of a privacy program should include:

- Internal and customer-facing privacy policies that address issues such as data collection, use and sharing practices, data security, and internal processes.
- Privacy by Design practices that encourage the development of systems that minimize the collection and storage of personal data, where appropriate; and the conducting of 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;
- An oversight program with responsibility for establishing policies and processes. (e.g., many companies have a Chief Privacy Office to coordinate these functions and train employees as needed.)
- Voluntary privacy programs and standards developed through collaborative public-private collaboration that could serve as a safe harbor while enabling companies to adapt to rapidly changing technology and market developments.
- Controls and policies for managing the sharing of personal data with service providers and third parties, including vendor management and APIs.

USTelecom supports the use of a collaborative process much like the one NIST used in developing the Cybersecurity Framework that incorporated input from industry and other

[4] Comments of USTelecom, *In the Matter of Developing the Administration's Approach to Consumer Privacy*, NTIA, Docket No. 180821780-8780-01, RIN 0660-XC043 at p. 6 (Nov. 9, 2018).

stakeholders. However, it is important to note that privacy is a different animal than cybersecurity. NIST should ensure that its Privacy Framework facilitates innovative and beneficial uses of data, such as the use of personal data for research and in order to develop new technologies, including Artificial Intelligence solutions, accompanied by the use of proper safeguards.

Furthermore, while NIST's prior work on government privacy engineering is to be applauded, we do not believe this work to be transferable to the Privacy Framework. The federal government's collection and use of data is governed by a completely different legal regime, including the Privacy Act, that does not apply to private sector companies.

That said, USTelecom's members agree that a worthwhile privacy framework necessarily requires appropriate security controls. Safeguards such as encryption, pseudonymization, enforceable codes of conduct, and security protections enable data use for socially beneficial purposes, while reducing risk of misuse or harm to individuals. The sensitivities that may be associated with identified data are mitigated when data is de-identified, aggregated, or does not otherwise identify a known individual, but through which insights can be derived to offer great benefits to consumers and society and such use. USTelecom members have long found success through use of best practices in the areas of data security and data de-identification. With proper use of these practices the risk associated with the use of personal data is effectively minimized. For example, data used for marketing purposes often is aggregated or anonymized to give consumers information and services they expect to receive from their service provider. Data de-identification reduces privacy risks, and in combination with aggregation, the amount of personal data that is available is also significantly reduced. Utilizing these sorts of techniques, is the best way to achieve reasonable safeguards while not impeding continued innovation.

USTelecom also supports a model for any framework that accounts for the burden of its applicability on smaller providers. Just as some companies operate solely within the United States and others operate globally, there are also companies serving rural parts of the U.S. that are considerably smaller than the larger companies that first come to the average consumer's mind.

US Telecom further notes that any framework for privacy risk mitigation must also take into account the need to not interrupt beneficial uses of information and innovation. As the Internet has grown up and become part of everyday commerce, consumers have come to expect that in order to engage in commerce and conduct everyday activities, such as making purchases, paying utility bills, signing up for activities, etc. requires the sharing of some non-sensitive information. NIST should be mindful of these facts and focus on creating a Privacy Framework that is voluntary, non-prescriptive and outcome based in such a way that harmonizes with existing, time-tested successful practices.

Respectfully submitted,

USTELECOM

B. Lynn Follansbee
Its Attorney

601 New Jersey Avenue, NW, Suite 600
Washington, D.C. 20001
202-326-7300

January 14, 2019