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

Dear Ms. MacFarland:

In response to the National Institute of Standards and Technology's ("NIST") recent request for information regarding the development of a privacy framework, I submit the below comments for consideration.

The advent of Europe's General Data Protection Regulation ("GDPR") in May 2018 represented a watershed moment in the regulatory landscape related to data privacy and cybersecurity. While European courts have long recognized an inherent right to privacy, only recently has that right come into conflict with an expansive (and growing) body of technologies that allow for greater data collection, storage, and processing than was ever thought possible. Consequently, technology companies around the world are struggling to bring existing data processing practices based on legitimate business objectives into compliance with laws like the GDPR. The problem is especially difficult for international companies which may be subject to a variety of conflicting data privacy laws in various jurisdictions, a common scenario in an increasingly e-commerce-based ecosystem. As a result, organizations seek industry-recognized frameworks to synergistically guide corporate governance, compliance, information security, and enterprise risk management functions. NIST's proposal of a privacy framework should therefore consider the following factors to help meet these objectives:

- **Voluntary participation**: In its information published online, NIST notes that the Framework is intended to be voluntary.[1] While regulatory approaches with one-size-fits-all requirements are rarely successful, any framework based on purely voluntary participation must confer a distinct benefit on participants in order to ensure industry buy-in. In short, there needs to be an incentive, beyond that of a comprehensive approach to ensuring privacy protections. The NIST Cybersecurity Framework ("NIST CSF") can serve as guidance here. For example, Ohio's recently released Senate Bill No. 220 provides that:

  A covered entity that implements and maintains a cybersecurity program that complies with the NIST cybersecurity framework, or other industry recognized framework … shall constitute an affirmative defense to any cause of action … that alleges the failure to implement reasonable cybersecurity control resulted in a data breach.[2]

  Thus, those who implement the NIST CSF can already use it as evidence of information security, which directly reduces potential legal and insurance costs

[1] https://www.federalregister.gov/documents/2018/11/14/2018-24714/developing-a-privacy-framework
[2] https://www.itgovernanceusa.com/blog/ohio-gets-breach-ready

ultimately passed on to consumers. The developing NIST Privacy Framework should confer similar advantages to participants as a recognized privacy controls framework.

- **Alignment with other standards**: To that end, the developing Framework needs to also align with existing understandings of privacy and data security risks to help guarantee adoption with any management systems already implemented. The GDPR and other subsequent privacy laws use the controller/processor distinction to help define what data rights and responsibilities apply to each party in the data supply chain. In addition, the Framework should ideally align with other "industry recognized" frameworks, much like the existing NIST CSF's alignment to ISO/IEC 27001. ISO/IEC 27001 is used as a risk-based approach to managing information security at nearly 39,500 organizations worldwide (1,517 in the U.S.); NIST CSF is used by more than 30% of organizations in the U.S.[3,4] The more any new framework can align across established approaches to enterprise risk management, the more likely it can be leveraged.

- **Risk-based approach**: In order to align with ISO/IEC 27001 and the NIST CSF, the NIST Privacy Framework should be risk-based to allow for flexible, cost-effective approaches to privacy protections. Many risk management frameworks base business decisions on objective analysis of corporate risk vectors to facilitate an evolving response to threats based on changes in the legal or technological landscape. In the short term, this allows for more cost-effective solutions as residual risks are operationalized; in the long term, ongoing risk management methods take on a consistent, objective approach that stabilizes over time.

- **How organizations define privacy risk**: Organizations often define "privacy risk" in ways which compete with consumer definitions and legal interpretations. Individuals often consider privacy risk as an affront to their personal boundaries, and the information that can provide detail about or beyond those boundaries. In contrast, organizations have historically considered privacy as an imperative to securing confidential business communications and trade secrets. Increasingly though, as technology companies found ways to monetize data that seemed mundane on their own, the mass collection of that data in the aggregate has allowed organizations to glean information about very private aspects of personal lives. Through compliance initiatives with laws like the GDPR, organizations are required to consider the personal impact of their business practices, taking into account the volume, velocity, and variety of data that is collected, processed, and stored. The important additional consideration is that current law generally only recognizes privacy risk when it materializes in actual damages. This economic loss doctrine fails to consider that privacy risk may not materialize in the moment, as identity theft is under no time restraint, and data once lost is not easily recovered. Subsequently, the NIST Privacy Framework should position privacy risk from the personal point of view, to help guarantee organizations continue to measure and

[3] https://www.iso.org/the-iso-survey.html
[4] https://www.nist.gov/industry-impacts/cybersecurity

mitigate privacy risk on an individual level. By focusing on the end user, personnel can work doubly to protect their privacy in online interactions at work and at home.

- **Organizational challenges to consider**: The strongest challenge to organizations looking to operationalize any compliance-based risk management approach is finding a scalable system that works across vertical silos that may differ in culture, cost appetite, and consumer markets. Therefore, the NIST Privacy Framework should do its best to approach privacy in an agnostic fashion with regard to technology so that protections can be applied regardless of what products collect data, or what internal systems process and store data. The approach also needs to be scalable for small and medium-sized organizations so that compliance projects do not represent an undue cost burden, effectively serving as a regulatory hurdle to overcome rather than a cost-effective approach to comprehensive protection.

As NIST continues to draft iterations of its anticipated privacy protections framework, it should also continue engaging industry stakeholders for input, and IT Governance USA is happy to help. We are a leading authority on data security and IT governance for business and the public sector. We help a variety of international organizations with data privacy and cybersecurity compliance issues, and our customer base spans Europe, the Americas, the Middle East, and Asia. As a result, we are intimately familiar with the challenges faced by organizations as they struggle to bring existing data processing practices into compliance with laws like the GDPR. Many of our international clients rely on industry-recognized frameworks to guide corporate governance functions. We therefore recommend that NIST's proposed privacy framework considers an incentivized, risk-based approach that aligns with existing standards to help provide a scalable, easily adoptable system to manage privacy risk for corporations and consumers alike.

Respectfully,

Alan Calder
Founder and Executive Chairman
IT Governance USA