HITRUST

855.HITRUST

www.HITRUSTAlliance.net

January 14, 2019

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

Sent via email: privacyframework@nist.gov

Re: **Developing a Privacy Framework**

Dear Ms. MacFarland:

On behalf of HITRUST®, I thank you for the opportunity to provide comment on NIST Request for Information dated November 14, 2018 *Developing a Privacy Framework; Document Number 1811011997-8997-01*. HITRUST looks forward to working with you and NIST on developing a workable privacy framework that balances the needs of industry and the rights of consumers.

Founded in 2007, HITRUST Alliance is a not-for-profit standards organization whose mission is to champion programs that safeguard sensitive information and manage information risk for organizations across all industries and throughout the third-party supply chain. In collaboration with privacy, information security and risk management leaders from both the public and private sectors, HITRUST develops, maintains and provides broad access to its widely adopted common risk and compliance management and de-identification frameworks; related assessment and assurance methodologies; and initiatives advancing cyber sharing, analysis, and resilience.

The foundation of all HITRUST programs and services is the HITRUST CSF®, a certifiable risk-based controls framework that provides organizations with a comprehensive, flexible and efficient approach to regulatory compliance and risk management. Developed in collaboration with information security professionals, the HITRUST CSF rationalizes relevant regulations and standards into a single overarching security framework. For example, the HITRUST CSF incorporates the HIPAA Privacy and Security Rules and the NIST *Framework for Improving Critical Infrastructure Cybersecurity*, or Cybersecurity Framework, and Version 9.2 also includes privacy controls based on internationally recognized privacy frameworks, including the Fair Information Practice Principles (FIPPs), the Organization for Economic Cooperation and Development (OECD) Privacy Principles, and the Asia-Pacific Economic Cooperation (APEC) Privacy Framework.

The HITRUST CSF also supports a risk-based approach to determining an entity's privacy and security posture. Leveraging the CSF, the HITRUST CSF Assurance Program provides organizations and their business associates with a common approach to managing security assessments that creates efficiencies and contains costs associated with multiple and varied assurance requirements. The HITRUST CSF Assurance Program includes risk management oversight and a rigorous assessment methodology governed by HITRUST and designed for the unique regulatory and business needs of various industries. When combined with the HITRUST CSF, the program provides organizations with a common approach to managing security assessments that creates efficiencies and reduces costs associated with multiple and varied assurance requirements.

HITRUST strongly applauds NIST's support of a risk-based approach to privacy. We strongly support NIST's work on the Cybersecurity Framework and believe it has helped industry improve its security posture; we believe a privacy framework document could serve the same purpose. As we have seen more broadly with security controls, there is a balance to be achieved between the risk involved and the resources it is commercially appropriate to dedicate to privacy policies and procedures. Additionally, HITRUST supports NIST's focus on a cost-effective approach that can be implemented across industries, company sizes, and existing legal and regulatory requirements.

Specific Responses to the Request for Information

Risk Management

There has been growth recently in the use of privacy impact assessments (PIAs) and similar tools to evaluate and consider privacy risks. As the European Union's General Data Protection Regulation (GDPR) has come into force, more entities are required to use PIAs for certain, potentially high-risk data processing. In the United States, privacy has long been thought of more as a compliance issue than a risk management issue. HITRUST strongly supports NIST's intention to help entities recognize the importance of risk-based, outcome-based privacy programs and implement appropriate controls.

Organizational Considerations

Privacy frameworks such as the FIPPs, the APEC Privacy Framework, and the OECD Privacy Principles are the foundational documents on which most privacy laws, regulations, and practices are based. HITRUST recommends that the NIST Privacy Framework development process should include a review of these frameworks to understand these key principles and how they could inform a modern, risk-based approach to privacy. In addition to their recognition internationally, these frameworks have helped a common privacy language to evolve over time, upon which NIST could build.

The greatest challenge in creating a cross-sector privacy standards document will be the same as the one faced in developing the Cybersecurity Framework – balancing the need for the document to be industry and size agnostic without making it so high level that it loses utility. HITRUST also anticipates sector-specific guidance and overlays similar to those seen with the Cybersecurity Framework will be needed to truly assist entities in implementing the Privacy Framework efficiently and effectively.

HITRUST believes an important consideration for the NIST Privacy Framework is to ensure that it recognizes the need for coordination between privacy and security personnel. Certainly NIST has supported this through its inclusion of privacy principles in a number of its security-focused documents. In order for privacy to truly become part of the overall entity risk management strategy, companies must have the right people at the table, including privacy professionals, security professionals, compliance professionals, technologists, and those familiar with the workflow and desired outcome of data collection and use in the company.

In order to provide value to entities, which is key to the adoption of a voluntary framework, the Privacy Framework must also be consistent with national and international standards. While the Privacy Framework should not mirror the GDPR, its controls must be developed with an awareness of the GDPR and the standards therein that are increasingly being adopted worldwide. For example, cross-border data transfers must be freely made in order to support our global digital economy; anything else stifles innovation and economic growth.

Including information regarding privacy engineering and its importance in implementing privacy by design should help advance recruitment of a knowledgeable and skilled workforce and ensure that more people, including but not limited to students who could pursue relevant education and company executives, are aware of this growing field and its utility.

Structuring the Privacy Framework

Because of the key considerations in development of systems that collect data, use of that data and the retention and destruction of any data, HITRUST recommends that NIST strongly consider the information life cycle as defined by NIST or based on existing representations in structuring the NIST Privacy Framework. This ensures that the variables found at each stage in the life cycle can be appropriately considered and analyzed. Additionally, as different personnel will often be more involved at various points in the life cycle, it is a useful structure to aid one’s implementation of the Framework.

A Framework structure similar to that in the NIST Cybersecurity Framework, looking at functions, categories, and subcategories will allow entities to take an organized and appropriate look at their privacy risks and practices.

Specific Privacy Practices

HITRUST strongly supports NIST’s focus on specific privacy practices, including de-identification. HITRUST’s De-Identification Framework discusses appropriate de-identification strategies and focuses on the expert method of de-identification, which is necessary to balance data privacy and data utility in an appropriate manner. De-identification is a key feature in national and international laws and frameworks, and its importance in privacy risk reduction is seen in the many laws that exempt de-identified data from certain requirements. HITRUST strongly believes that de-identification – both full anonymization and pseudonymization as appropriate – is one of the key best practices in data use and analysis. NIST must ensure that any controls or processes relating to de-identification require the use of proper and appropriate expertise. As we have seen throughout the internet era, re-identification of data someone deemed de-identified can be extremely easy. We must ensure a full risk analysis is considered during the de-identification process before data is used or released. The Texas Medical Records Privacy Act specifically prohibits re-identification; HITRUST recommends a similar provision that includes exemptions for authorized re-identification and re-identification done for public health or safety reasons. Fewer abuses would occur if there were clear consequences to unapproved re-identification.

While this may be part of NIST's reference to default privacy considerations, HITRUST believes NIST should specifically mention data minimization as a best practice. In line with the common saying that "data is the new oil," entities have tended to collect as much data as possible, assuming it will have value in the future or some not-yet-considered way. This practice increases privacy risks substantially; you cannot have a breach of information you do not have. Ensuring that entities are analyzing their workflows and use of data to, as a default, collect only data they plan on using for the purpose for which it was collected immediately reduces possible privacy risks.

HITRUST also believes these principles are applicable to the Internet of Things and similar technological advances. One of the weaknesses often cited regarding HIPAA is that it does not cover wearables that collect sensitive health information. Increasingly we are seeing concerns with the number of applications and other systems that collect geolocation data on their users. Consumer trust is necessary for these innovations to grow and to meet or exceed expectations on their benefits. Encouraging broad adoption of privacy protection objectives by NIST would result in more entities not currently under a regulatory regime to consider privacy risks and ways to protect personal data while still meeting consumer expectations for utility.

The most challenging practice to put in place for many entities is setting strong default privacy settings. As we have seen through responses to breaches from large technology companies, many existing products and services were not designed to allow granular consent or collect personal data in a way that labels it with the use for which it was collected. Without combating this challenge and growing the field of privacy by design, we will not see the substantial growth needed in privacy risk reduction worldwide.

We thank NIST once again for the opportunity to provide these comments, and look forward to working with you during the development of a privacy framework that balances business, international, and consumer needs and values.

Very truly yours,

Carl A. Anderson
Chief Legal Officer and Senior Vice President for Government Affairs