HITRUST

6175 Main Street
Suite 420
Frisco, TX 75034

855.HITRUST
(855-448-7878)
www.HITRUSTAlliance.net

November 9, 2018

David J. Redl
Assistant Secretary for Communications and Information
National Telecommunications and Information Administration
1401 Constitution Ave., NW
Washington, DC 20230

Sent via email: privacyrfc2018@ntia.doc.gov

Re: **Comments on *Developing the Administration's Approach to Consumer Privacy*, Docket No. 180821780-8780-01**

Dear Mr. Redl:

On behalf of HITRUST, I thank you again for the opportunity to provide comment on *Developing the Administration's Approach to Consumer Privacy* published in the Federal Register by the National Telecommunications and Information Administration (NTIA) on September 26, 2018. HITRUST looks forward to working with you and this Administration on developing a workable privacy framework that balances consumer protection with innovation as well as American ideals that still support international data exchange.

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 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.

The HITRUST CSF is a risk-based controls framework that incorporates the HIPAA Privacy and Security Rules and the NIST *Framework for Improving Critical Infrastructure Cybersecurity*, or Cybersecurity Framework. The most recent edition of the CSF 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.

6175 Main Street
Suite 420
Frisco, TX 75034

855.HITRUST
(855-448-7878)
www.HITRUSTAlliance.net

The United States' involvement in developing the FIPPs and its participation in the OECD and APEC processes demonstrates our country's commitment in this area. The CSF supports a risk-based approach to determining an entity's privacy and security posture. Additionally, we have seen many organizations recommend or require a CSF assessment from any third parties with which it is sharing consumer data.

The HITRUST CSF Assurance Program delivers simplified compliance assessment and reporting for HIPAA, HITECH, state, and business associate requirements. Leveraging the HITRUST CSF, the 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 the risk management oversight and assessment methodology governed by HITRUST and designed for the unique regulatory and business needs of various industries.

HITRUST strongly applauds the NTIA's support of a risk-based approach to consumer privacy. 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 security policies and procedures. This is particularly true, as the NTIA mentions, with respect to small and mid-sized businesses. There should not be unduly harsh requirements for all companies, when some take on more consumer data and more sensitive data than others.

HITRUST also agrees with the NTIA that the goal of a strong consumer privacy protection approach should be to consumers are reasonably informed about what data is being collected and why. As discussed in Section 3 of the Federal Trade Commission's (FTC) hearing 1 on Competition and Consumer Protection in the 21st Century, privacy-related torts and the resulting common law has long focused on the reasonable person standard. When providing personal data to companies, there must be sufficient transparency so that a reasonable person would understand how their information is being used and shared and such use and sufficient minimization of use so that any use or sharing is appropriate and commensurate to what a reasonable person would anticipate given the circumstances.

Specific Responses to the Request for Comment

A. Feedback on core privacy outcomes

The core privacy outcomes reflect the principles found in most privacy frameworks. More examples of means of transparency would likely be helpful to industry, as there is much debate in this area. HITRUST supports NTIA's focus on context when discussing the control outcome. Even the European Union's General Data Protection Regulation (GDPR) limits consumer rights depending on the basis on which information was obtained. If, for example, a professional email address and contact information is personal data that will be protected under the approach, businesses must know that they do not have to honor a deletion request of information if doing so would effectively prohibit the business from billing for products or services provided. HITRUST strongly supports the need for accountability to flow down from an organization that

6175 Main Street
Suite 420
Frisco, TX 75034

855.HITRUST
(855-448-7878)
www.HITRUSTAlliance.net

shares data with other third parties; adequate protection cannot be achieved if passing the data to an affiliate or a vendor releases all protection obligations.

B. Feedback on high-level goals

NTIA has chosen a strong list of high-level goals for a US consumer privacy protection system. What remains unclear is how the proposed approach would balance creating a harmonized approach while maintaining the sectoral system currently in place. A lack of legal clarity on what standards apply when and to whom an entity is accountable in terms of not just consumers but regulatory bodies would drastically undermine the success of any system. HITRUST strongly supports having a risk and outcome-based approach and agrees with NTIA that these approaches have been successful in the cybersecurity realm.

C. Comments on next steps and measures

HITRUST would strongly support encouragement and incentives from the Administration for entities to use existing risk-based privacy and security frameworks, such as the HITRUST CSF, to assess their data protection postures. This could be done through procurements and could be implemented quickly, since these tools are already on the market and in use. While HITRUST agrees that multiple stakeholders should be heard on commercial data privacy-related issues, it would encourage the NTIA to work with the FTC and NIST on ensuring that voices from all the entities' hearings are shared across the Administration.

D. Definitions of key terms

Terminology is a key area of concern in global data protection standards. HITRUST would strongly suggest that the NTIA consider defining consumer or user and their data.

It should be clear if this includes legal persons as well as natural persons and whether it includes the data of natural persons relating to their professional lives. As an example, the approach should clarify whether my email address, carl.anderson@hitrustalliance.net, is the type of data under consideration. While it does include my name, it is in the context of my work email account, and therefore not something generally considered private information in the United States. It must also be clear to what extent the framework would apply to aggregated information that has been de-identified in accordance with an expert approach, such as that discussed in the HITRUST De-Identification Framework.

Additionally, as a main focus of the approach is to reduce the likelihood of harm to the consumer or user, there should be a reliable definition of "harm." There has been discussion at privacy forums in the United States and abroad about what harms a privacy framework should attempt to alleviate. Privacy breaches can lead to psychological, physical, social, and economic harm. There is general agreement that economic and physical harms should be considered and the data subject appropriately compensated. There is some agreement that psychological and social harms that that occur due to a release of information that would be find highly offensive to a reasonable person should also be considered and appropriate compensation provided to the data

HITRUST
Health Information Trust Alliance

6175 Main Street
Suite 420
Frisco, TX 75034

855.HITRUST
(855-448-7878)
www.HITRUSTAlliance.net

subject. The question of whether non-physical or monetary harms caused by releases that would be highly offensive to the particular individual involved or just offensive to a reasonable person has less consensus should be addressed.

E. Changes with respect to the FTC

HITRUST would defer to the FTC on whether it needs change to resources, processes, or statutory authority to implement and enforce Administration's approach to privacy.

F. Global Adoption of the proposed outcomes and high-level goals

Global harmonization is extremely important to ensure the exchange of data internationally, which is a major component of the digital economy. Implementation of privacy and security processes and procedures occurs more efficiently and effectively if they can be implemented business-wide, which would require more consistency globally given the global marketplace and needs of multinational corporations.

We thank NTIA once again for the opportunity to provide these comments, and look forward to working with you as we continue to create an approach to consumer privacy that balances business, international, and consumer needs and values. Global harmonization of privacy practices that is flexible enough to respect the sovereignty of each nation and cultural norms on privacy is necessary for the continuation of the digital economy and for individuals to see the most value out of use of their data. The HITRUST CSF, with its focus on a strong, risk-based approach combining standards from US and international bodies, could serve as a tool for businesses to ensure they are following the approach to privacy taken by the Administration.

Very truly yours,

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