

From: Anne Kimbol <anne.kimbol@hitrustalliance.net>  
Sent: Thursday, October 24, 2019 10:53 AM  
To: privacyframework <privacyframework@nist.gov>  
Cc: Carl Anderson <carl.anderson@hitrustalliance.net>  
Subject: Privacy Framework comments

Attached please find HITRUST's comments on the preliminary draft of the NIST Privacy Framework. Thank you for the opportunity to comment and continue working with NIST, Anne Kimbol

Anne Kimbol

Asst. General Counsel

Privacy Officer

P: 469-269-1148 | E: anne.kimbol@hitrustalliance.net

CONFIDENTIALITY NOTICE: The contents of this email message and any attachments may contain confidential, proprietary or legally privileged information and/or may be subject to copyright or other intellectual property protection and be legally protected from disclosure. This information is intended only for use of the addressee or addressees named above for its intended purpose. If you are not the intended recipient of this message or their agent, or if this message has been addressed to you in error, please immediately alert the sender by reply email and then delete this message and any attachments. If you are not the intended recipient, you are hereby notified that any use, dissemination, copying, or storage of this message or its attachments is strictly prohibited.



6175 Main Street  
Suite 420  
Frisco, TX 75034

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

October 24, 2019

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

Sent via email: [privacyframework@nist.gov](mailto:privacyframework@nist.gov)

Re: **Comments on the Preliminary Draft of the NIST Privacy Framework**

Dear Ms. MacFarland:

On behalf of HITRUST®, I thank you for the opportunity to provide comment on the preliminary draft of the NIST Privacy Framework. HITRUST strongly applauds NIST's support of a risk-based approach to privacy and supports NIST's focus on a cost-effective approach that can be implemented across industries, company sizes, and existing legal and regulatory requirements.

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.

HITRUST continues to support NIST's work in developing the Privacy Framework, focusing on risk-based approaches, and ensuring the Framework is technology agnostic. While HITRUST applauds NIST's efforts, we believe there are remaining areas of potential improvement.

### ***General Comments***

HITRUST applauds NIST's efforts to create a privacy framework in response to the increased awareness of privacy among consumers and the need for businesses to respond accordingly. There is much uncertainty about privacy in the United States, not just legally but morally. With states passing or considering their own privacy laws and little movement in Congress of data privacy laws, the background against which privacy is analyzed in the United State is extremely blurry.

By choosing not to define personal data, privacy rights, or the level of control data subjects should have over their data, NIST has respected this uncertainly. Unfortunately, it also limits the value of the Privacy Framework. While processing of data that are authorized by law and contract are important, the Framework appears to assume the data has been obtained in a proper manner and may be used for the wanted purpose if proper controls are in place. This type of assumption has led to many of the privacy breaches, as defined for this purpose as a violation of what a reasonable consumer would believe the data could be used for, we are facing today. Without well-reasoned principles on the level of control consumers have over their data and how that impacts what businesses may do with their data, a privacy framework is incomplete.

In part because of the above, the Framework itself serves an only limited role in assessing a privacy program. An organization attempting to implement the Framework will have a difficult time knowing where to start, and those with low maturity in privacy may assume that the Framework covers their full programs. Additionally, because of the lack of key definitions and concepts, adoption of the Framework will look very different across organizations. This leaves those writing sector specific guidance to either fill in these holes or acknowledge them and limit the usability of that guidance as well. Even if sector specific guidance includes definitions of personal data and proper collection and use thereof, implementation across sectors will vary widely enough that compliance with the Framework will have little meaning.

Until these fundamental questions are addressed, HITRUST recommends NIST and organizations looking to adopt the Framework focus on standards already in place in the market and through international standards development organizations. By trying to be too inclusive, an admirable goal, NIST may have helped no one.

### ***Specific Comments on the Draft***

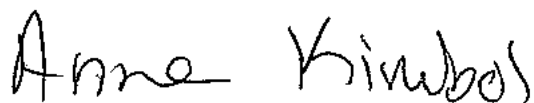
One of the stated goals of the Framework is to establish a common privacy vocabulary. While certain terms are already standard in the industry, organizations are not always defining them in the same way. NIST's approach of creating new terms that have not been used in the privacy world is unlikely to succeed at least in part because of international use of privacy terminology and work and its failure to match existing privacy regulations worldwide and standards work including, most pertinently, the International Standards Organization and International Electrotechnical Commission's Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines (ISO/IEC 27701:2019). HITRUST suggests NIST would have more success with their common language goal by using common terms and concepts such as processors and controllers (as opposed to third-party stakeholders), anonymization and pseudonymization (called disassociability in the Framework), and data processing as including data actions. Having clear definitions of existing terms, HITRUST believes, will increase the likelihood of adoption of a common language. Based on their previous standards, HITRUST feels ISO/IEC's 27701:2019 will be widely adopted globally, and opportunities to align the two standards are recommended.

Additionally, while the attempt to ease use of the Privacy Framework and Cybersecurity Framework is admirable, it has also unnecessarily complicated the Privacy Framework. Privacy and security certainly overlap, but they use different languages and different structures in terms of standards to reflect their unique focus.

HITRUST recommends that NIST clarify that privacy risk exists in offline data processing. This is particularly relevant in the healthcare industry, where faxes are still a common means of sharing sensitive patient data. Clarification about considering and potentially working with data subjects could also strengthen the Framework.

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. HITRUST respects that NIST has done yeoman's work in a very difficult area in the hopes of helping businesses and customers alike. We believe, however, that the overarching policy questions must be answered before such a Framework can successfully be created and implemented.

Very truly yours,



Anne Kimbol  
Chief Privacy Officer and Assistant General Counsel