HITRUST

6175 Main Street
Suite 420
Frisco, TX 75034

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

January 19, 2018

National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

Sent via email: cyberframework@nist.gov

Re: **Comments on Draft v2 of Version 1.1 of the Framework for Improving Critical Infrastructure Cybersecurity**

To Whom It May Concern:

On behalf of HITRUST, I thank you once again for the opportunity to provide comments on the pending update to the NIST *Framework for Improving Critical Infrastructure Cybersecurity* ("the NIST *Cybersecurity Framework*").

HITRUST also appreciates NIST's consideration and recognition of the efforts already undertaken in industry to leverage control frameworks. We believe there is wide support in industry for NIST to focus its efforts on establishing a uniform method of reporting while encouraging industries to tailor specific control frameworks and associated assurance programs to meet the needs of the industry.

As you know, the HITRUST CSF is one of the most widely used control-based information risk management framework in the healthcare industry and forms the basis for Healthcare and Public Health (HPH) sector implementation guidance[1] for the NIST *Cybersecurity Framework,* produced under the auspices of the Critical Infrastructure Protection Advisory Council (CIPAC). The use and leverage of control frameworks like the HITRUST CSF continue to receive wide adoption and these efforts should be encouraged.

Based on our long experience in helping organizations in the healthcare industry address cybersecurity-related legislation and regulation at the federal and state level, we offer the following comments to NIST on the proposed update to the *Cybersecurity Framework*.

Specific comments on the proposed update to the NIST *Cybersecurity Framework*

We note that many of the concerns raised in our comments on the initial draft of version 1.1 were addressed by NIST, and believe the new draft *Cybersecurity Framework* is a significant improvement. Subsequently we'll focus on the few outstanding issues that either remain or are particular to the second draft.

[1] Joint HPH Cybersecurity Working Group (2016). *Healthcare Sector Cybersecurity Framework Implementation Guide*. Available from the US-CERT Cybersecurity Framework Website at https://www.us-cert.gov/sites/default/files/c3vp/framework_guidance/HPH_Framework_Implementation_Guidance.pdf.

Executive Summary

Page 2, lines 147-148. We agree that NIST must "continue coordinating with the private sector and government agencies at all levels," and believe NIST should become more involved in the development and/or review of Sector-specific implementation guidance for the NIST *Cybersecurity Framework*.

Section 2.2 Framework Implementation Tiers

Pages 11-12, lines 408-415. NIST states, "Tiers are meant to support organizational decision making about how to manage cybersecurity risk, as well as which dimensions of the organization are higher priority and should receive additional resources. Progression to higher Tiers is encouraged when cost-benefit analysis indicates a feasible and cost effective reduction of cybersecurity risk." We agree in principle. However, consistent with the point made on risk tolerances in our comments on the initial draft, we believe progression to higher tiers may be required for compliance in some highly regulated industries, such as healthcare. Although the HIPAA Security Rule provides some latitude in implementation, the Rule generally requires covered entities and their business associates to select reasonable and appropriate safeguards (controls) that provide for the adequate protection of health information against all reasonably anticipated threats. Subsequently, progression to a higher Tier may be driven by the need for compliance rather than a cost-effective risk reduction.

Section 3.2 Establishing or Improving a Cybersecurity Program

Page 19, line 621. In Step 3, Create a Current Profile, we concur with NIST's observation that noting partial achievement of an outcome supports subsequent steps in the Framework's cybersecurity program improvement process but again note the guidance does not specify which steps or how they would be impacted. Recommend explaining how partial achievement impacts these steps.

Section 4.0 Measuring and Demonstrating Cybersecurity

Page 26, lines 830-831. NIST states, "Measuring the degree of implementation for controls catalogs or technical guidance listed as Informative References," which could be interpreted as meaning other control catalogs are excluded. As this is inconsistent with, *inter alia*, the statement on page 847, lines 854-856, suggest revising the statement to read, "… for controls catalogs or technical guidance, examples of which are listed as Informative References."

Page 26, line 833. It is not clear to us what is meant by "artificial indicators of current state and progress in improving cybersecurity risk management." What constitutes an artificial indicator (measure)? Suggest NIST define this term in the glossary or explain what is meant in the body of the text if organizations are mean to avoid their use.

HITRUST

6175 Main Street
Suite 420
Frisco, TX 75034

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

General comments on the proposed update to the NIST *Cybersecurity Framework*

Public-private partnership is important in this space.

> *Ensuring the protection and resilience of the nation's critical infrastructure is a shared responsibility among multiple stakeholders—neither government nor the private sector alone has the knowledge, authority, or resources to do it alone.*[2]

We would like to re-iterate the position, as stated in our comments on the initial draft of the proposed update, "that public-private partnerships like those demonstrated through the development and maintenance of the NIST *Cybersecurity Framework* are critical to the successful adoption and implementation of strong cybersecurity programs by industry…. [So we remain] concerned by the apparent lack of discussion—let alone emphasis—on sector-specific guidance like the *Healthcare Sector Cybersecurity Framework Implementation Guide* and ask why the role sector guidance plays in NIST *Cybersecurity Framework* implementation has [still] not been addressed. In essence, users of the NIST *Cybersecurity Framework* have nothing to 'connect the dots.' HITRUST strongly recommends NIST address this issue in the upcoming revision."

We thank NIST once again for the opportunity to provide these comments, and look forward to working with you as we continue to improve the state of critical infrastructure cybersecurity and data protection.

Very truly yours,

Dr. Bryan S. Cline, CISSP-ISSEP, CISM, CIPP/US
Vice President, Standards & Analysis

[2] https://www.dhs.gov/critical-infrastructure-protection-partnerships-and-information-sharing