HITRUST
Health Information Trust Alliance

6175 Main Street
Suite 420
Frisco, TX 75034

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

April 10, 2017

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

Sent via email: cyberframework@nist.gov

Re: Comments on Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity

To Whom It May Concern:

On behalf of the Health Information Trust Alliance (HITRUST), we thank you for the opportunity to provide comments on the pending 2017 update of the NIST *Framework for Improving Critical Infrastructure Cybersecurity* ("the NIST *Cybersecurity Framework*").

We applaud NIST for soliciting feedback from industry on this important framework. HITRUST believes that it is vitally important that we protect patients and their family members from cyber risks. As you go forward, we offer our cooperation, as well as our extensive experience in supporting the NIST *Cybersecurity Framework.*

Founded in 2007, the Health Information Trust Alliance (HITRUST) was born out of the belief that information protection should be a core pillar of, rather than an obstacle to, the broad adoption of health information systems and exchanges. HITRUST – in collaboration with public and private healthcare privacy and information security leaders – has championed programs instrumental in safeguarding health information, systems and exchanges while ensuring consumer confidence in their use.

HITRUST programs include the establishment of a common information risk and compliance management framework (HITRUST CSF); an assessment and assurance methodology; educational and career development; advocacy and awareness; and a federally recognized cyber Information Sharing and Analysis Organization (ISAO) and supporting initiatives.

The HITRUST CSF is the most widely used information risk management framework adopted in the healthcare industry and forms the basis for Healthcare and Public Health (HPH) sector implementation guidance[1] for the NIST *Cybersecurity Framework*, and has been leading the industry in cyber risk management, threat preparedness and response through initiatives such as the Cyber Threat Xchange – cyber threat intelligence sharing platform and CyberRX – industry and segment-specific threat preparedness and response exercises.

[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.

In fact, HITRUST has the most active cyber threat sharing platform in the industry, was the first to connect to the Department of Homeland Security's (DHS) Automated Indicator Sharing (AIS) program, and is the only healthcare organization currently sharing automated, bi-directional Indicators of Compromise (IOCs) with DHS. We also pioneered an Enhanced IOC program to address gaps in the collection and consumption of IOCs for healthcare organizations. We also recently testified before the House Homeland Security Committee on HITRUST programs, the benefits of information sharing, and the benefits of public-private partnerships.

HITRUST encourages NIST to consider and recognize the efforts already undertaken in industry to leverage control frameworks. The use and leverage of control frameworks continue to receive wide adoption and these efforts should be encouraged. 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 controls frameworks and associated assurance programs to meet the needs of the industry. One size does not fit all and many sectors already have begun to do so.

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*

Note to Reviewers on the Update and Next Steps

> Page iii, line 28 (and others). Reference is made to the "cybersecurity ecosystem" throughout the document without definition in context of the NIST guidance. One must refer to the original Department of Homeland Security (DHS) document, *Enabling Distributed Security in Cyberspace*,[2] to interpret what this means. Recommend defining the term in Appendix B and explaining what this means to an organization implementing the NIST *Cybersecurity Framework*, as appropriate, wherever the term is used.

Executive Summary

> Page 2, lines 114-117. NIST states the "use, evolution, and sharing of best practices of this voluntary Framework are the next steps to improve" our national cybersecurity. We're at a loss to understand how this is different from an organization implementing a controls-based risk management framework (RMF) like that promulgated by NIST via its SP 800-series documentation, which is one of many Illustrative References in the NIST *Cybersecurity Framework* Core that would provide the actual prescription necessary to implement the control objectives specified by the Core Subcategories. In fact, the HITRUST CSF and CSF Assurance Program provided the healthcare industry the ability to describe their current and target security postures, identify and prioritize improvement, assess progress toward the target state, and communicate risk and compliance among

[2] Available from https://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf.

internal and external stakeholders several years before the NIST *Cybersecurity Framework* was released in 2014. The real value of the NIST *Cybersecurity Framework* to industry is that it provides a common, yet comprehensive view of cybersecurity that focuses on organizational resilience rather than simply 'security.' As indicated in Section 2.2, Framework Implementation Tiers, industry must still determine the best practices needed for an organization to provide a minimally acceptable level of due diligence and due care, satisfy its regulatory compliance requirements, consistent with its business objectives, risk appetite, and specific risk tolerances.

Section 2.2 Framework Implementation Tiers

CMM®		NIST *Cybersecurity Framework*		Result
Level	Capability[3]	Level	Capability[4]	
5 Optimizing	Continuous process improvement is adopted and in place by quantitative feedback and from piloting new ideas and technologies.	4 Adaptive	The organization adapts its … practices based on lessons learned and predictive indicators…. Through a process of continuous improvement … the organization actively adapts to a changing cybersecurity landscape….	Quality / 'Securability' (Capability)
4 Qualitatively Managed	Processes are measured by collecting detailed data on the processes and their quality.	3 Repeatable	The organization's risk management practices are formally approved and expressed as policy. Organizational cyber practices are regularly updated based on the application of risk management processes….	
3 Defined	All processes are defined, documented, standardized and integrated into each other.			
2 Managed	Processes are established and there is a level of discipline in implementing the processes.	2 Risk-informed	Risk management practices are approved by management but may not be established as organizational-wide policy.	
1 Initial	Processes are ad-hoc, chaotic.	1 Partial	Organizational cybersecurity risk management practices are not formalized, and risk is managed in an ad hoc and sometimes reactive manner.	Risk

[3] Descriptions of the CMM levels are from http://www.vectorstudy.com/theories/capability-maturity-model.
[4] Language, limited to the risk management process, is taken from the Tier descriptions on pp. 10-11 of the proposed update to the NIST *Cybersecurity Framework*.

Page 9, lines 348-350. NIST states its Implementation Tiers "do not represent maturity levels." We disagree. The NIST *Cybersecurity Framework* Implementation Tiers—Partial, Risk-informed, Repeatable and Adaptive—are very similar to the original Capability Maturity Model® (CMM®) maturity levels—Initial, Managed, Defined, Qualitatively Managed, and Optimizing—as indicated in the above table.[5]

In fact, much of the language in Section 2.2 is consistent with a capability maturity model.

Where the Implementation Tiers appear to depart from the CMM's maturity levels is the NIST *Cybersecurity Framework*'s focus on four specific areas related to cybersecurity—Risk Management Process, Integrated Risk Management Program, External Participation, and Cyber Supply Chain Risk Management—as opposed to the CMM®'s more general focus on program management and process maturity. However, there's no question that an organization at a higher NIST *Cybersecurity Framework* Implementation Tier would generally have more cybersecurity capability (maturity) than an organization at a lower Tier.

Page 9, lines 352-356. We agree that "Tier selection and designation naturally affect Framework Profiles," but this relationship exists because the NIST *Cybersecurity Framework* Implementation Tiers are consistent with a capability maturity model. Subsequently, an organization is able to estimate its current Tier based on an assessment of the maturity of its HITRUST CSF implementation for relevant controls. In addition, the HITRUST CSF control requirements selected by an organization based on its specific organizational, system and regulatory risk factors help define its target profile and ultimately its desired Implementation Tier.

Section 3.0 How to Use the Framework

Page 14, lines 502-513. We find the addition of text around how the NIST *Cybersecurity Framework* (as a whole) can be applied in the Information Systems Security Engineering (ISSE) process incongruent with the high level of the Framework. At best, the control objectives specified by the Core Subcategories could be used to help inform the requirements elicitation process. Requirements for ISSE in system/service development and acquisition would be better addressed by one or more Core Subcategories (e.g., PR.IP-2 or similar).

Section 3.2 Establishing or Improving a Cybersecurity Program

Page 15, lines 543-544. In Step 1, Prioritize and Scope, the selection of a desired Implementation Tier could be used to "express varying risk tolerances," but we believe this has certain limitations in a heavily regulated industry. Although the HIPAA Security

[5] The basic table is adapted from http://www.askprocess.com/resources/articles/GlobalKnowledge/CMMI-Value.pdf.

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, the Tier's expression of an organization's risk tolerances is best understood when compared to a reasonable standard of due diligence/care, such as that provided by the HITRUST CSF for the healthcare industry.

Page 15, line 552. 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 note the guidance does not specify which steps or how they would be impacted. Recommend specifying how partial achievement impacts these steps, e.g., the remediation or corrective action planning process in Step 6.

Pages 15-16, lines 564-566. In Step 5, Create a Target Profile, how an organization should reflect characteristics of its desired Implementation Tier in its desired cybersecurity outcomes lacks explanation. Recommend NIST define these "characteristics" for the reader.

Section 4.0 Measuring and Demonstrating Cybersecurity

Pages 21-22, lines 744-768. HITRUST understands the subject of cybersecurity measures and metrics is a difficult one and applauds NIST's attempt at addressing it in the Guide. However, we find the treatment as written, here and in subsequent sections, may be somewhat obtuse for the average reader. For example, it's difficult to discern from the discussion about measures and metrics in lines 748-755 why metrics are associated with Implementation Tiers, Categories and Subcategories and measures are associated with the Informative References. The reason is the References provide examples of controls that support the cybersecurity objectives specified by the Subcategories, and measures would most likely be defined at this level. Examples of such measures from Black et al. (Mar 2009)[6], referenced on line 750, include the percentage of desktops with antivirus installed and the percentage of antivirus installations with current virus definitions (p. 5). By then aggregating or combining these individual measures, one can generate metrics at the Subcategory level. Another example occurs in lines 756-761, where NIST states leading measurement is preferred to lagging measurement when evaluating a business outcome. However, the terms leading and lagging are relative to where the measurement is in a particular process. If a metric exists for the business outcome, then by definition the cybersecurity measurement used as an input into the business metric would be leading. But it is also lagging in the sense this metric may be related to a NIST Category, which in turn may be derived from metrics for its underlying Subcategories. In general, we believe the readability and subsequent usefulness of this and related sections can be significantly improved.

[6] Cybersecurity Metrics and Measures, Black et al., March 2009, available from http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=51292.

Section 4.1 Correlation to Business Results

Page 21, lines 770-811. NIST states the purpose of measuring cybersecurity is to correlate it with business objectives so that it may "understand and quantify cause-and-effect." Unfortunately, correlation does not always equate to causality, typically due to the confounding of multiple variables. We also find it concerning that the discussion does not address the many issues that make cybersecurity measures and metrics problematic, unlike the discussion in Black et al. (Mar 2009), which specifically addresses known problems with accuracy and the selection and use of measures. The rest of this section is less problematic, especially as the discussion remains focused on correlation rather than cause-and-effect. However, HITRUST recommends NIST take a similar approach to Black et al. (2009) in its discussion of Cybersecurity measurement.

Section 4.2 Types of Cybersecurity Measurement

Page 23, line 814. Reference the table, NIST identifies the measurement type for specific risk management processes, such as those found in the Section 3.3 of the NIST *Cybersecurity Framework*, as 'measure.' While we agree that measures can be developed for a process, so too can metrics.

> *The term metric is often used to refer to the measurement of performance, but it is clearer to define metrics and measures separately. A measure is a concrete, objective attribute, such as the percentage of systems within an organization that are fully patched, the length of time between the release of a patch and its installation on a system, or the level of access to a system that a vulnerability in the system could provide. A metric is an abstract, somewhat subjective attribute, such as how well an organization's systems are secured against external threats or how effective the organization's incident response team is. An analyst can approximate the value of a metric by collecting and analyzing groups of measures. (Black, et al., 2009, p. 2)*

Providing assurances to a third party using a Current Profile, as described in Section 3.3, would constitute a metric rather than a measure. This is because the results may be provided qualitatively or quasi-quantitatively based on an assessment of its level of compliance with controls supporting the Subcategories in the Profile. Recommend updating the table to reflect the possibility that both measures and metrics may be collected for 'Process,' as the "corresponding framework component" is currently described. Implementation Tiers are also referenced in Section 3.3, lines 601-604, which according to the table are associated with metrics under 'Practices' vice "Process,' and subsequently may cause additional confusion for the average reader.

Page 23, lines 821-823. NIST specifically states that practices are composed of discreet processes, which makes the measurement categories in the table problematic since 'Practices' and 'Process' are no longer mutually exclusive. A practice necessarily has processes associated with it, as do management and technical measurement. The latter are also confusing, since not all the controls in the informative references are technical controls. Some are administrative or management controls, and others are physical. It appears NIST's view of management measurement is based on, or similar to, general performance measurement[7] (perhaps specifically to object-oriented performance measurement), whereas technical measurement is based on, or similar to, technical performance management.[8] Whether or not this interpretation is correct, HITRUST recommends NIST reconsider the classification schema and/or provide additional guidance on the subject (e.g., definitions, examples) to provide the clarity needed.

Page 24, lines 852-862. HITRUST agrees that—barring a textbook risk analysis and specification of a custom set of controls—an underlying control framework is essential for an organization to implement the cybersecurity objectives specified by the Core Subcategories. However, we believe the statement that these references "offer detailed measures" is inaccurate, as an organization must still identify/select or develop measures for each control it implements. This position is substantiated in lines 854-862.

Appendix A: Framework Core

Page 25, lines 864-866. The HITRUST CSF is one of the most widely adopted security controls frameworks in the industry. Given that healthcare is said to be as much as 1/5th of the U.S. economy and the HITRUST CSF is extensible beyond the healthcare industry (as demonstrated by its application to business associates that also serves other industries, e.g., Cloud service providers), HITRUST CSF controls should be included in the NIST *Cybersecurity Framework* Core's Informative References.

Responses to the specific questions asked by NIST on the proposed update to the NIST *Cybersecurity Framework*

Are there any topics not addressed in the draft Framework Version 1.1 that could be addressed in the final?

Recommend NIST incorporate guidance on how to use control frameworks like NIST SP 800-53 and the HITRUST CSF to implement cybersecurity programs consistent with the guidelines in the NIST *Cybersecurity Framework*. It should also address the role of the Critical Infrastructure Protection Advisory Council (CIPAC),[9] the Government Coordinating Council (GCC), Sector Coordinating Council (SCC),[10] GCC/SCC sector-specific joint working groups,[11] and the sector-specific *Cybersecurity Framework* implementation guidance documents, which are generally made available to the public on

[7] For example, see https://cio.gov/performance-metrics-and-measures/ or https://www.hrsa.gov/quality/toolbox/methodology/performancemanagement/.

[8] See https://dap.dau.mil/acquipedia/Pages/ArticleDetails.aspx?aid=7c1d9528-4a9e-4c3a-8f9e-6e0ff93b6ccb.

[9] See https://www.dhs.gov/critical-infrastructure-partnership-advisory-council for more information.

[10] For more information on the Government and Sector Coordinating Councils, see https://www.dhs.gov/cipac-charters-and-membership.

[11] See https://www.dhs.gov/cipac-working-groups-critical-infrastructure-sector for more information.

the DHS US Computer Emergency Response Team (US-CERT) *Cybersecurity Framework* Website.[12]

How do the changes made in the draft Version 1.1 impact the cybersecurity ecosystem?

Third-party assurance is well-understood if not always well-implemented by industry, and supply chain security has been addressed by several security control frameworks, including ISO/IEC 27001:2013, *Information technology – Security techniques – Information security management systems – Requirements*, NIST SP 800-53 and companion 800-series documentation, and the HITRUST CSF. However, HITRUST believes the additional focus on supply chain security at the NIST *Cybersecurity Framework*'s overarching level provides the emphasis and direction needed by organizations that do not currently leverage these types of control frameworks, or know to leverage guidance in NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*.

For those using Version 1.0, would the proposed changes impact your current use of the Framework? If so, how?

No, the HITRUST CSF integrates and harmonizes multiple legislative, regulatory, and best practice frameworks relevant to the healthcare industry, including ISO/IEC 27001:2013 and NIST SP 800-53, which addresses much of the guidance provided in NIST SP 800-161 about supply chain risk management. The HITRUST CSF Assurance Program also leverages the maturity model outlined in NISTIR 7358, *Program Review for Information Security Management Assistance (PRISMA)*, and addresses industry best practices for the use of measures and metrics as part of an enterprise-wide continuous monitoring program.

For those not currently using Version 1.0, does the draft Version 1.1 affect your decision use the Framework? If so, how?

We do not foresee the changes proposed for v1.1 will have a significant impact on current interest or the current rate of adoption by HIPAA covered entities and business associates.

Does this proposed update adequately reflect advances made in the Roadmap areas?

The proposed update to the NIST *Cybersecurity Framework* does not adequately address the progress made by industry in conformity assessment. The *Healthcare Sector Cybersecurity Framework Implementation Guide* provides a model approach to the integration of a security control framework to support implementation of the NIST *Cybersecurity Framework*, including an approach to defining measures for the controls in

[12] Nine sector-specific guides are currently available from the US-CERT Website: https://www.us-cert.gov/ccubedvp/cybersecurity-framework#framework-guidance.

the framework, and how to compute and communicate performance metrics, including estimates for NIST Implementation Tiers.

Is there a better label than "version 1.1" for this update?

Incorporation of supply chain risk management and the use of measures and metrics is a significant update to the NIST *Cybersecurity Framework* and warrants designation as v2 vice v1.1.

Based on this update, activities in Roadmap areas, and activities in the cybersecurity ecosystem, are there additional areas that should be added to the Roadmap? Are there any areas that should be removed from the Roadmap?

Recommend NIST add implementation support for the NIST *Cybersecurity Framework* to the Roadmap. Part of this guidance would necessarily address the need to integrate the guidance contained in the NIST *Cybersecurity Framework* to Sector-specific guidance developed under the auspices of Critical Infrastructure Protection Partnerships and the Critical Infrastructure Protection Advisory Council (CIPAC).[13]

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

Guidance should allow for the most efficient and effective deployment possible.

HITRUST has seen significant interest by industry in the NIST *Cybersecurity Framework* but there's also significant confusion about its implementation. Many organizations try to implement the NIST *Cybersecurity Framework* without using an underlying control framework like NIST SP 800-53 or the HITRUST CSF, and subsequently struggle to determine the security controls needed to achieve the NIST *Cybersecurity Framework*'s objectives. NIST should clarify and stress the need for organizations to select controls based on a traditional risk analysis or leverage a relevant control framework—such as those identified in the Core's Informative References—to allow for the most efficient and effective *Cybersecurity Framework* implementation possible.

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.*[14]

[13] For more information, see https://www.dhs.gov/critical-infrastructure-protection-partnerships-and-information-sharing.

[14] Ibid.

HITRUST agrees with DHS 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. In fact, HITRUST worked collaboratively with the U.S. Congress as it developed language contained in the Cybersecurity Information Sharing Act (CISA), which directs the Department of Health and Human Services (HHS) to "establish, through a collaborative process with NIST, DHS, Federal and private sector partners, a common set of voluntary, consensus-based, and industry-led guidelines"[15] consistent with the NIST *Cybersecurity Framework*. But we are 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 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 for the opportunity to provide these comments regarding the critically important issue of cyber security and data protection, and look forward to working on making them a success.

Very truly yours,

Daniel Nutkis
Chief Executive Officer

[15] Cybersecurity Information Sharing Act (CISA), H.R. 2029—742, §405(d). Available from https://www.congress.gov/114/bills/hr2029/BILLS-114hr2029enr.pdf.