

April 21, 2022

National Institute of Standards and Technology
ATTN: Katherine MacFarland
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

VIA THE [FEDERAL ELECTRONIC RULEMAKING PORTAL](#)

Re: Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management – [RFI-2022-03642](#)

Dear Ms. MacFarland:

Please accept the following in response to NIST RFI-2022-03642, which requests public comment on a potential draft of the NIST Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework) and other potential standards, guidelines, and other information, including those relating to improving cybersecurity in supply chains.

Use of the NIST Cybersecurity Framework

1. The usefulness of the NIST Cybersecurity Framework for aiding organizations in organizing cybersecurity efforts via the five functions in the Framework and actively managing risks using those five functions.

The Core is arguably the most useful—and subsequently most widely used—part of the NIST Cybersecurity Framework. The Framework’s Core Functions, Categories, and Sub-categories help ensure organizations—regardless of size, industry, or geography—address a wide range of threats to the sensitive information they process. However, the five Core Functions are less useful in helping organizations actively manage their risks, as the lowest levels of the Core are Subcategories, which only provide desired cybersecurity outcomes, and Informative References, which provide “specific sections of standards, guidelines, and practices... that illustrate a method to achieve the outcomes associated with each Subcategory” [[NIST \(2018, Apr 16\). Framework for Improving Critical Infrastructure Cybersecurity v1.1](#), p. 7]. But HITRUST believes this works as intended, as it ‘forces’ organizations to design controls and/or select them from one or more Informative References and—as the Informative References are illustrative and not meant to be collectively exhaustive—other viable sources.

Unfortunately, the current version of the NIST Cybersecurity Framework does not fully explore how Informative References should be used. Instead, the document simply states, “organizations should determine which standards, guidelines, and practices, including those that are sector specific, work best for their needs” ([Ibid.](#), p. 15).

Since the need for a risk analysis to support control specification is the hallmark of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule (HSR) [[HHS \(2010, Jul 14\). Guidance on Risk Analysis Requirements under the HIPAA Security Rule](#), p. 1], the Joint HPH Sector Cybersecurity Working Group (WG)—a group chartered under the [Critical Infrastructure Partnership Advisory Council](#) (CIPAC) in 2014—published a

healthcare and public health (HPH) sector-specific guide in 2016 on implementing the NIST Cybersecurity Framework ([Joint HPH CWG \(2016, May\). Healthcare Sector Cybersecurity Framework Implementation Guide v1.1](#)). The guidance leverages control framework-based risk analysis [[Cline, B. \(2017, Sep\). Leveraging a Control-based Framework to Simplify the Risk Analysis Process, ISSA Journal 15\(9\)](#), pp. 39-42) to help organizations easily specify the controls required for their Target Profile ([Healthcare Sector Cybersecurity Framework Implementation Guide v1.1](#), pp. 18-19.) A second version of the sector guide—produced under the new Healthcare and Public Health (HPH) Sector Coordinating Council ([HSCC Cybersecurity WG](#))—is currently being put through the Department of Health and Human Services ([HHS](#)) review, approval, and release process by the Office of the Assistant Secretary for Preparedness & Response ([ASPR](#)) as joint [SCC](#) and Government Coordinating Council ([GCC](#)) guidance.

It is only by specifying controls based on a traditional risk analysis approach such as the one articulated by NIST or a control framework-based approach leveraging the NIST Cybersecurity Framework’s Informative References (and similar resources) that an organization can determine how they will achieve the outcomes specified by the Framework’s Core Subcategories. And this is why NIST should explicitly address this issue in its next revision of the Cybersecurity Framework.

2. Current benefits of using the NIST Cybersecurity Framework. Are communications improved within and between organizations and entities (e.g., supply chain partners, customers, or insurers)?

As indicated in our response to the first question, one of the hallmarks of the NIST Cybersecurity Framework is the articulation of a broad range of cybersecurity outcomes via the Core Subcategories, as this provides the proverbial ‘Rosetta stone’ for organizations to communicate the state of their cybersecurity programs regardless of the unique risks they may face. However, there is no reliable indicator of whether the controls specified by an organization to address the Framework’s outcomes are reasonable and appropriate for an organization and provide adequate protection for its sensitive information (i.e., manage its cybersecurity risk within acceptable levels).

Implementation Tiers could potentially help communicate this risk, but they are somewhat limited in scope as they currently focus on the risk management process, integrated risk management program, and external participation by an organization [[NIST \(2018, Apr 16\)](#), p. 9]. However, we believe the focus areas could be expanded to include other areas of interest and discuss this further when addressing Cybersecurity Supply Chain Risk Management (CSCRM) later in our response.

Does the Framework allow for better assessment of risks, more effective management of risks, and/or increase the number of potential ways to manage risks?

HITRUST recognizes that NIST intended the Cybersecurity Framework to support the assessment of risk.

... the cybersecurity outcomes of the Framework Core support self-assessment of investment effectiveness and cybersecurity activities in the following ways:

- ...
- *Measuring the degree of implementation for controls catalogs or technical guidance listed as Informative References. ([Ibid](#), p. 20)*

However, the NIST Cybersecurity Framework could allow for better assessment and management of risk if the gap between outcomes and the controls needed to address those outcomes can be related to an organization's unique risks and risk appetite and tolerances. That said, the level of analysis needed to address this issue is currently—and should probably remain—outside the scope of the Framework.

HITRUST believes that viable approaches to communicating this risk exist in the private sector. Examples include a new approach being developed by the [FAIR Institute](#) based on its quantitative Factor Analysis for Information Risk (FAIR) model for very targeted types of risk questions (e.g., how much risk is reduced by implementing a specific control or corrective action) and HITRUST's new quasi-quantitative approach to residual risk analysis—which also leverages the results of an organization's control gap assessments—that provides a more 'triage' level of risk assessment that could be used to answer broader questions around risk (e.g., how do the cybersecurity investments I make this year reduce my overall exposure to a specific type of threat such as ransomware). The model also categorizes risk based on a standardized approach to calculating risk capacity for an organization, which allows organizations to view risks expressed as a monetary value in the context of their own organization's risk appetite and tolerances.

As for increasing the number of potential ways to manage risks, the overarching nature of the NIST Cybersecurity Framework already provides organizations wide latitude in how they manage cybersecurity risk.

What might be relevant metrics for improvements to cybersecurity as a result of implementation of the Framework?

Relevant metrics are problematic. Measuring adoption of any methodology is generally limited to either (1) survey research that elicits stakeholder opinions about the state of adoption and its impact on desired outcomes or (2) observational studies based on objective evidence of the same. Both approaches have their limitations.

For example, survey research is categorized as a descriptive research design [Leedy, P. & Ormond, J. (2005). *Practical research: Planning and design* (8th ed.)], which makes it much more difficult to make conclusions about causal relationships than in experimental research designs [Shadish, W., Cook, T., & Campbell, D. (2002). *Experimental and quasi-experimental designs for generalized causal inference.*] Observational studies are similarly non-experimental and have the same limitation. And, in both types of studies, obtaining access to appropriate personnel within multiple organizations is problematic in and of itself. In HITRUST's 15 years of experience in assessing and facilitating the sharing of cybersecurity assessment results with various private and public sector stakeholders, we believe it would be similarly difficult to obtain this type of information for any type of NIST Cybersecurity Framework adoption metric.

Despite these problems, HITRUST believes that a metric could be developed and that some organizations would be willing to provide relevant information. However, the metric would obviously suffer from a significant amount of self-selection bias as well as potential issues with construct validity and overall reliability [Carmines, E. & Zeller, R. (1979). *Reliability and Validity Assessment*]. Assertions of causality and generalization beyond the sample population would also remain difficult as well [[Shadish, W., Cook, T., & Campbell, D. (2002). *Experimental and quasi-experimental designs for generalized causal inference.*]

3. Challenges that may prevent organizations from using the NIST Cybersecurity Framework or using it more easily or extensively (e.g., resource considerations, information sharing restrictions, organizational factors, workforce gaps, or complexity).

All the examples presented in the question remain challenges for organizational adoption of the NIST Cybersecurity Framework, or any methodology innovation for that matter. Studies for similar methodologies, e.g., quality improvement and information systems security engineering, have shown that there are five principal factors related to successful adoption: leadership support, organizational culture, implementation planning, available resources for implementation, and training in the methodology, with leadership support being the most critical as it greatly effects the other listed factors [[Cline, B. \(2009\). An Implementation Process and Factor Model for Information Systems Security Engineering](#)].

4. Any features of the NIST Cybersecurity Framework that should be changed, added, or removed. These might include additions or modifications of: Functions, Categories, or Subcategories; Tiers; Profile Templates; references to standards, frameworks, models, and guidelines; guidance on how to use the Cybersecurity Framework; or references to critical infrastructure versus the Framework's broader use.

Risk analysis-based selection of controls from the NIST Framework Core's Informative References should be addressed in an existing Core Subcategory or a new one should be added to specifically address this objective (outcome). In this way, organizations will also ensure the controls used to achieve the remaining Core Subcategory's outcomes are reasonable and appropriate as well as provide more reliable assurances to stakeholders about the state of their cybersecurity programs. The expansion of Categories and Subcategories to address other specific areas of interest such as CSCRM, embedded systems (e.g., Internet of Things, IoT; Supervisory Control and Data Acquisition, SCADA, systems; and the integration of cybersecurity with enterprise risk management) may also be warranted. Implementation Tiers could also be expanded to include other focused areas in risk management such as CSCRM.

5. Impact to the usability and backward compatibility of the NIST Cybersecurity Framework if the structure of the framework such as Functions, Categories, Subcategories, etc., is modified or changed.

HITRUST's recommendations for changes to the Framework Core in the previous section will improve useability of the Framework while maintaining backwards-compatibility with prior versions.

6. Additional ways in which NIST could improve the Cybersecurity Framework or make it more useful.

Recommend providing additional guidance on how Implementation Tiers can be used to improve an organization's cybersecurity risk profile.

We know that a proper risk analysis will specify the controls needed to achieve the outcomes described by the Framework's Core Subcategories in a way that is 'risk-appropriate' for that organization. But it is the Implementation Tiers that provide additional context around the rigor with which the organization manages risk.

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 could receive additional resources.
[[NIST \(2018, Apr 16\)](#), p. 8]

For example, suppose two organizations—one small with low inherent risk and another large with high inherent risk—build risk management programs tailored to their unique circumstances. An evaluation of their respective

controls might indicate both programs are well implemented. However, evaluating their controls against the Tier definitions would likely indicate the larger organization with more risk has a more ‘mature’ approach to risk management than the smaller, less risky one. Yet both are appropriate to the respective organization.

However, Implementation Tiers provide additional value by helping organizations understand when it is appropriate to add controls. This is because, as the NIST Cybersecurity Framework specifically states, moving from one tier to another should happen when a cost-benefit analysis indicates a feasible and cost-effective reduction of cybersecurity risk. [ibid.] In other words, we demonstrate a positive return on investment (ROI) when we do so.

An organization must estimate how much it costs to implement controls and the subsequent reduction in risk to calculate ROI. The cost of implementation is not hard to do. (Organizations do it all the time.) Valuing the risk reduction, however, is more difficult. As mentioned earlier in our response to Question 2, HITRUST is currently developing an approach to quasi-quantitative residual risk analysis that will help organizations value these risk reductions in monetary terms, and the FAIR Institute offers another approach to the same. Other approaches likely exist as well.

Adding the use of Implementation Tiers in this way with the support of quasi-quantitative residual risk analysis or similar approach would certainly help organizations make valid, cost-effective decisions about how they improve their cyber risk management program by implementing controls that support higher Implementation Tiers when a positive return on investment exists.

Relationship of the NIST Cybersecurity Framework to Other Risk Management Resources

7. Suggestions for improving alignment or integration of the Cybersecurity Framework with other NIST risk management resources. As part of the response, please indicate benefits and challenges of using these resources alone or in conjunction with the Cybersecurity Framework. These resources include:

- *Risk management resources such as the NIST Risk Management Framework, the NIST Privacy Framework, and Integrating Cybersecurity and Enterprise Risk Management (NISTIR 8286).*
- *Trustworthy technology resources such as the NIST Secure Software Development Framework, the NIST Internet of Things (IoT) Cybersecurity Capabilities Baseline, and the Guide to Industrial Control System Cybersecurity.*
- *Workforce management resources such as the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity.*

Risk Management Frameworks

Since the NIST Cybersecurity Framework is an overarching or ‘umbrella’ framework that exists over other risk management frameworks, HITRUST views them as complementary in that the NIST Cybersecurity Framework helps facilitate communication of risk information between and amongst organizations that may use these disparate risk management frameworks. However, HITRUST recommends NIST develop guidance on relating or integrating these frameworks in the same way it provides guidance on how Informative Resources—generally control-based—help organizations achieve the outcomes specified by the Framework’s Core Subcategories vis-à-vis the Online Informative Reference (OLIR) program.

Trustworthy Technology Resources

Trustworthy Technology Resources should be used to inform (1) how an organization implements related controls, (2) define new controls to address related NIST Cybersecurity Framework Core Subcategories, (3) help NIST identify new Subcategories in relevant Categories or new Categories and supporting Subcategories, and/or (4) identify new focus areas for the NIST Cybersecurity Framework's Implementation Tiers and develop supporting requirements for each Tier. (Note this response is similar to our response to Question 14.)

Workforce Management Resources

Workforce management resources should be implemented 'alone' rather than in conjunction with the NIST Cybersecurity Framework. We see no value in using them in the Framework itself.

8. Use of non-NIST frameworks or approaches in conjunction with the NIST Cybersecurity Framework. Are there commonalities or conflicts between the NIST framework and other voluntary, consensus resources?

The NIST Cybersecurity Framework MUST maintain compatibility with non-NIST frameworks and approaches to remain true to its original vision of facilitating communications between organizations and improving the state of cybersecurity within these organizations. There is obvious compatibility between the NIST Framework and non-NIST control frameworks like the CIS CSC, ISO 27001/2, and the HITRUST CSF, as they provide a library of control requirements from which organizations can draw upon to address the NIST Cybersecurity Framework Core Sub-categories. Compatibility also exists with non-NIST risk management approaches such as HITRUST's quasi-quantitative residual risk analysis (QRRRA) methodology or the FAIR Institute's factor analysis of information risk (FAIR) as well as other voluntary, consensus resources such as the HICP or the HPH Sector Cybersecurity Framework Implementation Guide. This is because the NIST Cybersecurity Framework focuses on what outcomes organizations' need to address/achieve and these other resources show how organizations can achieve these outcomes. Changing this dynamic would weaken rather than strengthen the utility of the NIST Cybersecurity Framework.

Are there commonalities or conflicts between the NIST framework and cybersecurity-related mandates or resources from government agencies?

Cybersecurity-related mandates are inherently conflicting with the NIST Cybersecurity Framework due to its voluntary, consensus-driven nature. However, such mandates could be perceived as requirements for specific controls that support various outcomes specified by the Framework's Core Subcategories. Resources provided by government agencies, however, are another matter as they may be leveraged on a voluntary basis consistent with the intent of the NIST Cybersecurity Framework. Resources may be selected based on the needs of an organization in the same way an organization is free to select the controls it believes are reasonable and appropriate for the outcomes specified by the Core Subcategories or the level of specific Implementation Tiers it chooses to adopt.

Are there ways to improve alignment or integration of the NIST framework with other frameworks, such as international approaches like the ISO/IEC 27000-series, including ISO/IEC TS 27110?

No. Alignment via the OLIR library is sufficient.

9. There are numerous examples of international adaptations of the Cybersecurity Framework by other countries. The continued use of international standards for cybersecurity, with a focus on interoperability, security, usability, and resilience can promote innovation and competitiveness while enabling organizations to more easily and effectively integrate new technologies and services. Given this importance, what steps should NIST consider to ensure any update increases international use of the Cybersecurity Framework?

Continue to maintain the outcome-level nature of the NIST Cybersecurity so that it complements rather than competes with other national and international cybersecurity control and risk management frameworks, whether in the private or government sector.

10. References that should be considered for inclusion within NIST's Online Informative References Program. This program is an effort to define standardized relationships between NIST and industry resources and elements of documents, products, and services and various NIST documents such as the NIST Cybersecurity Framework, NIST Privacy Framework, Security and Privacy Controls for Information Systems and Organizations (NIST Special Publication 800-53), NIST Secure Software Development Framework, and the NIST Internet of Things (IoT) Cybersecurity Capabilities Baseline.

HITRUST offers no specific recommendation around the inclusion of other cybersecurity control and risk management frameworks, standards, guidelines, or best practices as informative references vis-à-vis the NIST OLIR program. Rather, any framework, standard, or set of best practices used by an organization to help achieve the outcomes specified by the NIST Cybersecurity Framework Core Subcategories should be mapped, either informally by an owner or using organization or formally through the NIST OLIR program.

Cybersecurity Supply Chain Risk Management

11. National Initiative for Improving Cybersecurity in Supply Chains (NIICS). What are the greatest challenges related to the cybersecurity aspects of supply chain risk management that the NIICS could address?

Arguably the greatest challenge to improving cybersecurity throughout the supply chain is the ability of organizations to share third-party risk information with each other, whether in an organizations immediate supply chain or downstream of the supply chain. Problems that need to be addressed include but are not necessarily limited to:

- Scope of assessment
- Rigor of assessment
- Independence of assessment
- Standardization of reporting (format)
- Standardization of risk information
- Information sharing permissions
- Automated electronic exchange

How can NIST build on its current work on supply chain security, including software security work stemming from E.O. 14028, to increase trust and assurance in technology products, devices, and services?

No comment.

12. *Approaches, tools, standards, guidelines, or other resources necessary for managing cybersecurity-related risks in supply chains. NIST welcomes input on such resources in narrowly defined areas (e.g., pieces of hardware or software assurance or assured services, or specific to only one or two sectors) that may be useful to utilize more broadly; potential low risk, high reward resources that could be facilitated across diverse disciplines, sectors, or stakeholders; as well as large-scale and extremely difficult areas.*

No comment.

13. *Are there gaps observed in existing cybersecurity supply chain risk management guidance and resources, including how they apply to information and communications technology, operational technology, IoT, and industrial IoT?*

NIST should provide additional guidance on when it is appropriate to share information and what types of information should be shared up and downstream of an organization’s immediate suppliers. All technologies that potentially impact the confidentiality, availability, or integrity of information are relevant to the discussion around CSCRM and any guidance or resources that NIST subsequently provides.

In addition, do NIST software and supply chain guidance and resources appropriately address cybersecurity challenges associated with open-source software?

No comment.

Are there additional approaches, tools, standards, guidelines, or other resources that NIST should consider to achieve greater assurance throughout the software supply chain, including for open-source software?

No comment.

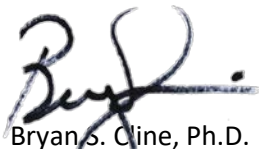
14. *Integration of Framework and Cybersecurity Supply Chain Risk Management Guidance. Whether and how cybersecurity supply chain risk management considerations might be further integrated into an updated NIST Cybersecurity Framework—or whether and how a new and separate framework focused on cybersecurity supply chain risk management might be valuable and more appropriately be developed by NIST.*

CSCRM is like any other aspect of an organization’s risk management program and should be integrated similarly into the NIST Cybersecurity Framework.

- CSCRM guidance can and should be used by organizations to inform implementation of the controls used to achieve the cybersecurity outcomes specified by the NIST Cybersecurity Framework’s Core Subcategories.
- CSCRM control frameworks can be used to inform the modification of existing NIST Cybersecurity Framework Core Categories and/or Subcategories or the addition of new ones
- CSCRM frameworks and guidance should not be used to modify the NIST Cybersecurity Framework’s Core Functions, as they are modeled on risk management and incident response processes: *identify* and *protect* information, and *detect, respond to, and recover* from cybersecurity incidents. Changing or adding to the Core Functions to ‘accommodate’ specific topics of interest such as SCRM, IoT, SCADA, or Enterprise Risk Management (ERM) would negatively impact the Core Functions value in helping organizations manage risk effectively.
- CSCRM frameworks and guidance should be used to add another area of focus to the NIST Cybersecurity Framework’s Implementation Tiers.

Thank you again for the opportunity to comment on these very important issues. Please feel free to contact me at Bryan.Cline@HITRUSTAlliance.ORG should you have any questions or desire any additional information related to our response.

Sincerely,

A handwritten signature in black ink, appearing to read "Bryan S. Cline". The signature is fluid and cursive, with a horizontal line extending from the end.

Bryan S. Cline, Ph.D.
Chief Research Officer