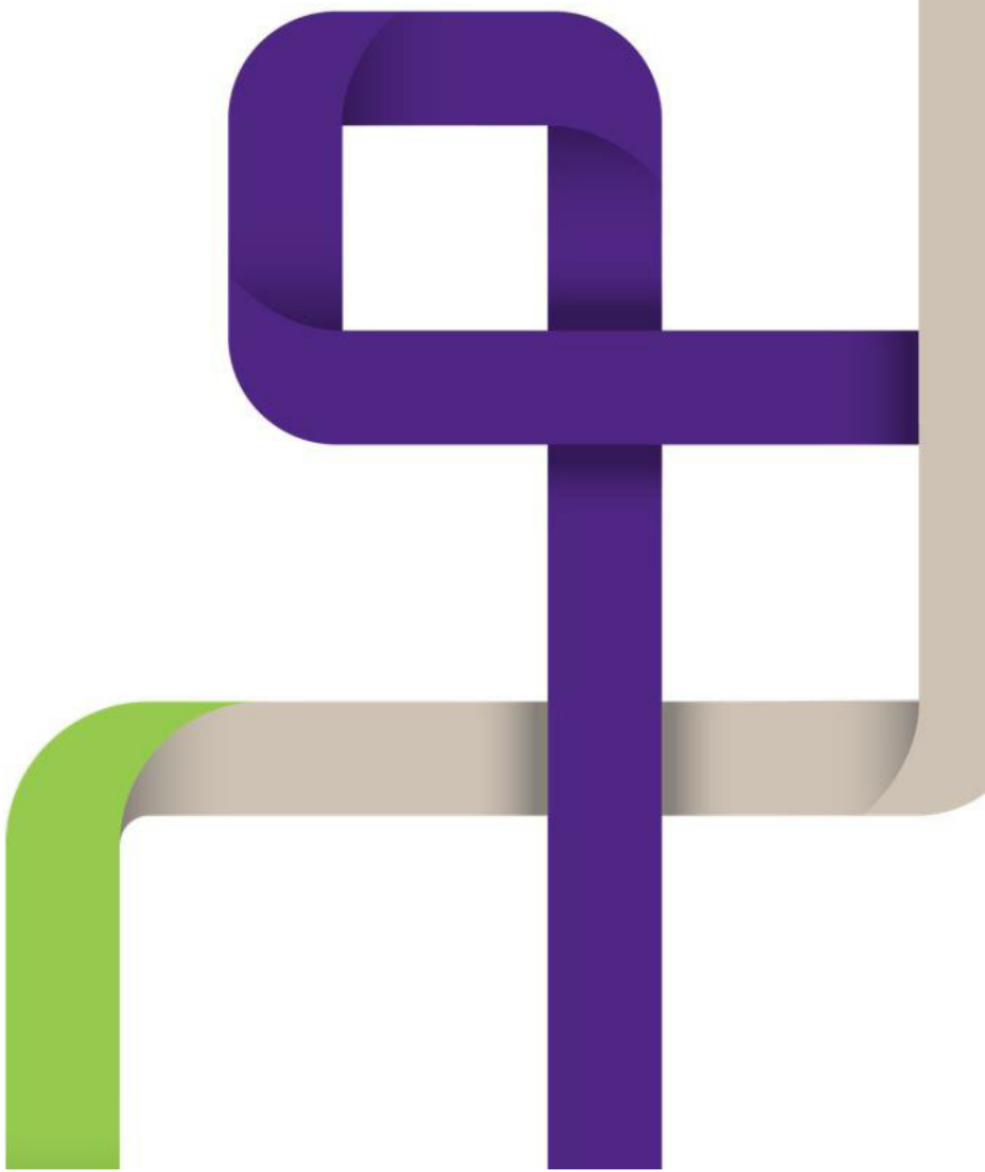
Grant Thornton

National Institute for Standards and Technology (NIST) Cybersecurity RFI

Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

April 25, 2022



NIST

Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

Prepared for:

NIST
Cybersecurity Framework
ATTN: Katherine MacFarland
100 Bureau Drive
Stop 2000
Gaithersburg, MD 20899

Prepared by:

Grant Thornton

1000 Wilson Boulevard
Suite 1400
Arlington, VA 22209
www.grantthornton.com

April 25, 2022

Point of Contact:

Dave Simprini, Principal

[redacted]

On January 1, 2020, Grant Thornton LLP ("Grant Thornton LLP" or "Parent"), a federal government contractor since 2001, reorganized its Public Sector service line into a wholly-owned subsidiary named Grant Thornton Public Sector LLC. All of the assets and personnel associated with Grant Thornton LLP's government practice (except for its government financial audit and attest practice that will remain with the Parent) have been transferred to the new subsidiary, Grant Thornton Public Sector LLC. The government is currently considering approval of novation of the transferred assets, including transferred contracts.

Grant Thornton LLP and Grant Thornton Public Sector LLC have entered into a Services Agreement, which provides for the two entities to provide assistance to each other on government contract opportunities and engagements.

Grant Thornton Public Sector LLC

Response to NIST Cybersecurity RFI

Grant Thornton's responses below are based on previous experience and lessons learned supporting federal and state governments and the private sector. We are eager to support continued dialogue and brainstorming sessions on this initiative so that NIST can advance the process of transforming ideas into actionable results. We look forward to the prospect of continued outreach and engagement on NIST cybersecurity and supply chain risk management initiatives.

Use of the NIST Cybersecurity Framework (CSF)

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.

Alignment of the NIST CSF to the five functions in the framework is a remarkably effective means to communicate at all levels (and technical competencies) of an organization. The logical continuum of Identify, Protect, Detect, Respond, and Recover helps frame cyber issues in a business context. We have applied the CSF functions in several ways including developing analytics and visualization tools, designing training curricula, and aligning our consulting services to our customers. For example, Grant Thornton developed a Cyber Analytics dashboarding tool using data extracted from the NIST CSF. We started by performing a series of cyber risk assessments utilizing the State of Florida Agency for State Technology (AST) FCS Risk Assessment Tool which can be found on the NIST CSF Resources Page under SLTT Resources. Once the risk assessments were complete, we aggregated results into a dashboarding solution so that our client could obtain an overview of cyber risk at the Function Level (Identify, Protect, Detect, Respond, Recover) or drill down into granular views at the Category or Sub-Category level.

An Extract, Transform, and Load (ETL) process was built through R and developed a word vector to analyze trending issues within the remediation recommendations description. To assess the sentiment and narrow our analysis to negative recommendations, the data was processed through RapidMiner for sentiment analysis. The result was a dynamic visualization and analytic tool using Tableau software as an overlay. This allowed clients to interact and facilitate data-driven decision-making with their cyber risk data. The Tableau dashboard created automated business intelligence reports for easily understandable and actionable enterprise decision-making with a specific focus on CSF functions.

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

   The strength of the CSF is its breadth and depth and plethora of amplifying guidance included in the NIST SP 800 series documents. For commercial organizations, the CSF is a fantastic framework when implemented correctly. It serves as a solid cybersecurity risk management platform that can consistently categorize risks and issues – strategic and tactical - across all tiers of an organization. As such, the CSF excels as an internally facing cybersecurity risk management, communications, and planning tool.

   The CSF can also blend with other disciplines to include budget formulation and execution activities to plan and track cybersecurity and IT investments that align to organization cybersecurity mitigation, maturity, and modernization activities. Budget formulation and execution can be consistently tracked across the five functions of the CSF providing organizations with a methodology to track performance and trends.

   Because the framework is voluntary, it is challenging to leverage it as a tool for external due diligence (e.g., supply chain risk assessments, insurance, etc.). Other frameworks that are audited have higher degrees of trust/priority since they are verified by a certified third party positioned to verify the design and effectiveness of controls in scope.

   Another strength of the CSF is its flexibility. Organizations can develop and implement a wide array of tactical, strategic, and compliance-oriented metrics that align to any level of the CSF. Our experience has shown clients who leverage the CSF as a strategic tool for measuring enterprise cybersecurity maturity receive the largest benefit. To that end, we encourage NIST to develop guidance and training material focusing on establishing metrics that emphasize CSF maturity across all levels and functions.

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).

   A primary challenge that prevents organizations from fully utilizing the CSF is a tendency to focus on the System Level (Tier 3) issues using the NIST RMF and NIST 800-53 control baseline rather than focusing on the Enterprise (Tier 1) or Department/Mission (Tier 2) environments. System-level focus is important to identifying and mitigating system-level risk. Organizations tend to be less experienced at aggregating, synthesizing, and developing risk mitigation strategies that look holistically across the enterprise. The result is sub-optimized mitigation strategies that may not align with IT modernization strategies, reduced purchasing power for mitigation or modernization investments, and inefficient use of FTE time within the organization to address stove-piped solutions.

A second challenge is that the use of the CSF is voluntary, so there is also some degree of prioritization toward a system-level focus rather than looking at the big picture. Mandatory frameworks or frameworks that require third-party audits often review management's engagement with cybersecurity / risk management issues increasing recognition, awareness, and adoption of these frameworks either by choice or regulation. Third-party audited frameworks (and their supporting vendor ecosystems) tend to do a better job providing guidance and support for the implementation of requirements, tools, and accelerators to optimize their business processes, and a variety of training programs/platforms for practitioners at all levels to learn. We recommend NIST consider bolstering the CSF with more training and support material for common business use cases designed to meet challenging cybersecurity scenarios.

A third challenge, related to the second challenge above, is that mandated frameworks will command the attention of organizations over voluntary frameworks. The federal government has many frameworks required by various industry-based regulations. Harmonizing these requirements with the NIST CSF as the foundation would ensure a common baseline is in place, and each industry-specific regulation may have its own unique overlay. This would accomplish two outcomes. First, a common baseline across all industries is established. Second, organizations with multiple regulatory requirements can maximize their compliance investments.

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.

   NIST CSF Maturity Tiers (1. Partial, 2. Risk-Informed, 3. Repeatable, 4. Adaptive) are similar to, yet not identical to the OIG FISMA Maturity Levels (1. Ad Hoc, 2. Defined, 3. Consistently Implemented, 4. Managed and Measurable, 5. Optimized). It would be useful if these maturity level scales were aligned for a 1-to-1 comparison. This would be especially useful in helping agencies establish a targeted, future-state profile that would not only improve the cyber posture of the organization but have the additional benefit of improving FISMA compliance scores in an “apples-to-apples" baseline.

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.

   Alignment of the NIST CSF to the five functions in the framework is a highly effective means to communicate at all levels (and technical competencies) of an organization. The logical continuum of Identify, Protect, Detect, Respond, and Recover helps frame cyber issues in a business context and is accessible to most audiences. Changes at the function level would be highly impactful as organizations that have adopted the CSF have oriented governance, oversight, and management functions around them. We encourage NIST not to modify the

five functions of the CSF. Changes at the functional level would negatively impact organizations that have adopted or plan to adopt the CSF. It will require significant rework and modification to internal business processes / reports that are designed around the current five functions.

Changes to categories and subcategories will also be impactful. However, there is more tolerance and flexibility at these lower levels as various control families and disciplines have evolved since the publishing of the CSF v. 1.1, to include improvements in privacy, supply chain, secure software design, and enterprise risk management. Changes at this level are necessary for the framework to continue being a leading and relevant framework for all types of organizations.

To minimize the impacts limiting usability and backward compatibility, we recommend NIST limit changes to the lowest levels of the CSF as possible. Next, a mapping document with a rationale should be published for public comment before implementation. Finally, finalized ample guidance and training should be provided explaining the context and rationale for the change to the CSF.

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

   The combination of the CSF framework core, maturity tiers, and profiles (both baseline and target) is a powerful tool in helping organizations improve their overall cyber posture. Some ideas on how to improve its effectiveness include:
   - Stronger emphasis on using the CSF at the Organization and Mission level vs. the system-level
   - Alignment of the maturity tiers to FISMA maturity levels
   - Provide and/or solicit more input to develop the library of use cases, tools, templates, and accelerators on the NIST CSF website
   - More universal mapping and harmonization of critical infrastructure frameworks
   - NIST needs to lead the charge in driving control harmonization
   - Need to evolve the framework to incorporate more privacy concepts
   - SCADA / ICS may have some limitations

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.

In general, the more integration and compatibility between the CSF and key NIST products like NISTIRs and IoT. A critical factor is ensuring that the integration is not a one-way proposition. In other words, the CSF should provide overlap and mapping to these frameworks and vice versa.

One area where we see significant opportunity for improved integration is the NICE Framework. Through the 5 Functions, the CSF provides a logical foundation for aligning workforce knowledge, skills, and abilities (KSAs) and may serve to assess the readiness of an organization's cyber workforce. This can be further aligned to organizational transformation initiatives to capture the process and technology baselines that can also be aligned to the 5 functions.

In the current state, the CSF and NICE frameworks provide limited integration and only include minor footnotes or references to one another. For integration to be truly effective, NIST should consider adding informative appendices or resources to both the CSF and NICE guidance and/or online resource repositories.

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

   Without question, the NIST Cybersecurity Framework and the ecosystem of supporting NIST special publications like SP 800-53, SP 800-37, and SP 800-39 are gold standards for cybersecurity programs of all shapes and sizes. The outcome-oriented guidance is provided in a manner that can be consumed by a variety of audiences and serves as a solid foundation for other organizations to explicitly reference or heavily borrow for their regulatory needs.

   In many cases, other frameworks (ISO 27001, PCI, CIS Top 20 CSC, SOC1/2, IRS 1075, FFIEC, HIPAA) are complementary to the NIST CSF. In practice, basing a cybersecurity program squarely on the NIST CSF positions organizations to successfully comply with other common frameworks with limited re-work or duplication of effort. The differences in the frameworks are often oriented around very specific control implementations that are borne out of broader legislative or industry requirements. For example, IRS 1075 and HIPAA prescribe record retention requirements for covered entities. The NIST CSF defers to legal

and regulatory requirements. This approach provides for maximum flexibility and a pathway for broad adoption of the CSF.

A second difference is related to the synchronization and update cycles of the various frameworks which creates periodic conflict. For example, when NIST published password change requirements in SP 800-63B back in 2017, encouraging the use of passphrases and shifting away from time-based password rotation. Organizations that adopted that guidance came into direct conflict with PCI's password controls requiring password rotation every 90 days. The PCI Security Standards Council may reconcile its framework with NIST guidance. In the meantime, the requirements do not align.

Finally, frameworks like ISO 27001, FFIEC, and IRS 1075 are conceptually aligned to the NIST CSF. However, these frameworks are audited by third parties. Frameworks that are audited by third parties often review management's engagement with cybersecurity / risk management issues increasing recognition, awareness, and adoption of these frameworks either by choice or regulation. As a result, these frameworks (and their supporting vendor ecosystems) tend to do a better job providing guidance and support for how to effectively meet these requirements. We recommend NIST consider bolstering the CSF with more training and support material for common business use cases designed to meet challenging cybersecurity scenarios.

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?

   International cooperation is important when balancing cybersecurity risk and the investments firms must make to meet their risk and compliance requirements. Harmonizing the global landscape of various cybersecurity requirements, to the greatest extent possible, positions firms to meet or exceed requirements effectively while delivering their goods and services. NIST should consider the following initiatives to continue improving collaboration with international standards and regulatory bodies.

   First, creating an inventory and mapping of major international standards with the CSF, as has already been done for the CSF v. 1.1 and frameworks like ISO 27001, are helpful for organizations to understand the relationship of the CSF to frameworks they may have already invested or considering for implementation. NIST can encourage this by facilitating voluntary submissions from host nations or even crowd-sourcing mappings through trusted channels.

   Second, NIST can take a leadership role and facilitate international conferences with international standards bodies and major regulators to discuss emerging trends in the cybersecurity framework community. These conferences could become incubators for

shared projects and initiatives that all participants and their constituents would benefit from. The broad adoption of video conferencing technologies over the past three years has the potential to greatly reduce costs and increase participation.

Finally, a practical barrier to international adoption is language translation. NIST should consider reproducing its documentation and key training material in an array of foreign languages to reduce the barrier to adoption internationally.

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

    NIST has a deep resource repository of publicly available tools, templates, and guidance. A more holistic linking of other reference material will help clearly demonstrate how NIST material can and does effectively support other legislative requirements, voluntary frameworks, and industry best practices.

    We recommend NIST consider collating and cross-referencing all Federally produced cybersecurity and privacy content (e.g., regulatory requirements and guidance) with related NIST material. For example, including crosswalks between NIST material and the FFIEC, IRS 1075, and HIPAA would be helpful for a variety of stakeholders that must comply with multiple frameworks.

    NIST should also consider integrating State-based requirements into the references program. This will help stakeholders that must meet state and Federal requirements to more easily understand how to tailor the cybersecurity and risk programs in an optimized manner.

    Finally, we recommend expanding the references program to include sanitized / anonymized use cases that demonstrate the real application of the CSF in making business decisions. This could be paired with publicizing, spreading awareness, and requesting input from industry to more frequently update the site with use case examples for continued learning and understanding.

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? 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?

The greatest challenges NIICS might address with regards to cybersecurity aspects relevant to current and emerging supply chain risk(s) include monitoring key suppliers beyond the immediate 3rd party. This means monitoring and scoring (and testing) cyber risk profiles for various supplier segments and according to various supplier engagements, out to the 4th, 5th, and 6th tiers. This underwriting evaluation needs to apply to all relevant cyber domains subject to qualified critical dependency assessment(s) and 24/7 monitoring considerations contingent upon the sensitivity of the data, the underlying processes, and overall operations inherent within the supply chain ecosystem. The analysis also needs to score and remediate any concerns related to confidentiality, integrity, and availability of critical supplier data sets as per established data governance best practices. Doing this would solve for:

- Lack of visibility into 4th and 5th parties and unknown risk blind spots
- Monitoring of risk domains in a way that is no longer manual, static, and siloed
- Resolution of unknown vendor concentration risks that otherwise leads to single-threaded supply chain issues with significant potential for lost revenue, data loss, fines and penalties, in addition to theft of intellectual property or other national secrets
- Easier pre-acquisition due diligence/equity acquisition
- Proactive merchant evaluation across multiple risk categories with continuous monitoring once in the network

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?

- There is an opportunity to further refine cybersecurity assessments to consider software DevOps and the assurance of code deployed within any operational environment.
- Pre-existing, unidentified, or inherent vulnerabilities are compounded by the constant need (at varying frequencies) to update firmware, which also further varies across device types. Even with regard to devices designed to update regularly, manufacturers do not always provide clear and readily available information on how to update the firmware. Users may not be able to discern whether the firmware is up to date. For devices with firmware that is not cryptographically signed and secure, devices may be updated from unsigned code, meaning that firmware could be rewritten without requirements for verification from the user. As such, firmware updates, especially those relevant to supply chain risk management and national security objectives, present major logistical challenges. IT individuals and accountable leaders need to be able to independently verify critical security information and therefore, must go beyond simply 'relying on" information solely provided by vendors.
- Firmware on items such as network cards, Wi-Fi adapters, and USB hubs are often not properly signed with either public or private keys. These devices need a process to verify that the operating firmware is authentic and can be trusted.
- As an example, see here for an active attack vector requiring an immediate solution: https://www.armis.com/research/tlstorm/

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.

    Grant Thornton, along with our partner Interos.io software, provides clients with an AI-enabled third-party risk management resiliency command center with data connections, risk identification, real-time prioritization, and mitigation plan deployment. The use of ML/AI to redefine how risk is underwritten also implies that risk is understood better. Key cyber risk variables are discerned, validated, weighted, scored, and mitigated according to criticality – and this can be done on a near-time basis without over-reliance on email notification or other manual processes. Suppliers can be scored, notified, and issues adjudicated in an entire underwriting ecosystem designed by Grant Thornton's Strategic Risk practice and in collaboration with our cyber security federal team.

    We protect leading organizations and the CIA triad from critical disruptions, while reinventing how companies manage business relationships. Fortune 100 companies use Grant Thornton/Interos -- in conjunction with a Cyber Scoring solution -- to triage newly reported breaches, hunt for potential cyber threats, and collaborate better with other functional teams requiring their time and expertise, namely supply chain cyber risk management. Using an arsenal of natural-language AI models, trained on supply-chain data, we've built a highly connected, multi-dimensional network of B2B relationships. We continuously monitor global events providing real-time indicators of supply chain vulnerability and distress, across any business ecosystem, and out to the Nth tier.

    Benefits include:

    1. Identify and investigate Nth party breaches. Cyber teams can instantly see Nth party relationships (e.g., SolarWinds, Log4j) and collaborate with internal/external contract holders (i.e., suppliers) to remediate impacts faster

    2. Assume a proactive vs. reactive risk posture - Continuous monitoring and better, more complete data allows for the discovery of emerging risk, particularly when used with an external additive Cyber Scoring solution like (RiskRecon)

    3. Collaborate better with internal stakeholders – A single platform allows for the consolidation of separate solutions to help bridge traditional bank silos, especially when an investigation or proactive assessment is needed

    4. Answer executive questions about cyber risk with more confidence - Board-level inquiries about global events and cyber threats require a constant response

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

Yes, and there are software tools/commercial enterprises that help suppliers (of all sizes) enable enterprise features in any SaaS app with just a few lines of code. They are able to Integrate SAML, Audit Logs, Privacy Vault, and Role Based Access in minutes. This is open-source and free. The link, https://github.com/boxyhq, provides an example of a organization solving this issue with regards to small suppliers, especially those who are veteran/minority-owned and often require quick assistance to achieve compliance with federal contracting (FAR et al) standards.

Further, NIST should move beyond zero trust by improving supply chain security. Zero trust is concerned with network architecture, but it does not account for a vendor's R&D functions or the security of its controllers, batteries, displays, hard drives, or other components.

To improve supply chain security, organizations must ask suppliers challenging questions: How can we perform ongoing checks to ensure that a vendor is reliable and has appropriately reduced the risk associated with its products? Does the vendor participate in vulnerability disclosure and management programs? How is it handling our data? How does it transport its goods from the factory to the point of assembly?

Zero trust should extend to open-source technology. It's often assumed these platforms are free from software errors because everyone can see the open-source code. Despite mostly positive reviews, open-source software isn't perfect. It can contain errors, and patching services are not necessarily included with the firmware/software. Organizations should refrain from integrating any open source software into their products without bona fide verification (see our answer #1, above).

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.

    This is the equivalent of asking about a fraud framework, or (pick your risk) any performance-based risk management framework, which is all in effect operational risk frameworks of varying types. It is confusing to the marketplace to develop frameworks that do not logically nest together as part of an integrated operational ecosystem. As such, the public (and corporate shareholders) are best served by one integrated governance framework designed to encapsulate and sole for all underlying risk types – across the operational domains. This is not only recognized by the Committee of Sponsoring Organizations (COSO, 2019) but by many leading global industries (Financial Services, Insurance, Asset Management, Manufacturing, Technology, et al). Further, there is the risk of confusing assurance and audit stakeholders, who have a role in reviewing and testing

both the 1st and 2nd Lines of Defense and assessing all operational risk types. Instead, a mapping between the NIST CSF and related 800-53, et al controls can be developed to align with and inform the Operational Risk Management framework which, otherwise currently contemplates supply chain risk.

One of the downsides of over fragmenting risk management functions is breeding unclear roles and duties for any one risk program's risk ownership. For instance, supply chain risk management is not typically owned or controlled by the cyber team at government, not for profit, or even private/commercial entities. The supply chain is often managed by a procurement team responsible for overseeing the entirety of supplier life cycle risks within the entirety of the supply chain, and of which cyber is only one such risk within their overall governance domain. It is more appropriate to integrate the NIST CSF into the procurement/supply chain operational risk function and align cyber risk and performance interests under the operational risk paradigm than to otherwise try to integrate the entirety of the supply chain world into the cyber risk management domain through the use of a "cyber for supply chain" domain. These business duty/line duty considerations are extremely relevant when considering the modern enterprise/modern government and how to effectively (reliably and validly) build a risk intelligent enterprise through integrated risk management pathways under an overarching (operational risk) governance framework. Saying it another way,' the cyber tail should not wag the tail of the entirety of the supply chain risk management dog".

This proposal is the work of Grant Thornton Public Sector LLC, the wholly owned subsidiary of Grant Thornton LLP, the U.S. member firm of Grant Thornton International Ltd, and is in all respects subject to negotiation, agreement, and signing of specific contracts. The information contained within this document is intended only for the entity or person to which it is addressed and contains confidential and/or proprietary material. Dissemination to third parties, copying, or use of this information is strictly prohibited without the prior written consent of Grant Thornton Public Sector LLC.

"Grant Thornton" refers to the brand under which the Grant Thornton member firms provide assurance, tax and advisory services to their clients and/or refers to one or more member firms, as the context requires. Grant Thornton International Ltd (GTIL) and the member firms are not a worldwide partnership. GTIL and each member firm is a separate legal entity. Services are delivered by the member firms. GTIL does not provide services to clients. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions.

Tax Professional Standards Statement

This document supports Grant Thornton LLP's marketing of professional services and is not written tax advice directed at the particular facts and circumstances of any person. If you are interested in the subject of this document, we encourage you to contact us or an independent tax advisor to discuss the potential application to your particular situation. Nothing herein shall be construed as imposing a limitation on any person from disclosing the tax treatment or tax structure of any matter addressed herein. To the extent this document may be considered to contain written tax advice, any written advice contained in, forwarded with, or attached to this document is not intended by Grant Thornton to be used, and cannot be used, by any person for the purpose of avoiding penalties that may be imposed under the Internal Revenue Code.

GT.COM