Response to the NIST Request for Information to gather information about evaluating and improving cybersecurity resources for the cybersecurity framework and cybersecurity supply chain risk management

Carnegie Mellon University
Software Engineering Institute
CERT Division

April 2022

The following is a non-exhaustive list of possible topics that may be addressed in any comments. Comments may address topics in the following list, or any other topic believed to have implications for the improvement of the NIST Cybersecurity Framework or NIST's cybersecurity guidance regarding supply chains. NIST will consider all relevant comments in the development of the revised Framework and guidance regarding supply chains.

Note: NIST RFI text is in black, SEI response in red.

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 CSF is less useful to small- to mid-sized organizations, particularly those without dedicated cybersecurity staff. Often, such organizations do not know what questions to ask to determine if they are implementing a CSF subcategory effectively. Additional guidance that includes questions drawn from control frameworks might enhance adoption in smaller organizations, because the current informative references can be problematic for them. One approach that could be useful is to offer a version of the CSF that translates practices in the CSF to a question format.

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?

   A. The CSF provides extensive benefit to cybersecurity management and communications on risk among organizations. To further improve communications and clarify technical and cybersecurity terminology, it may be valuable for NIST to provide expanded leadership on establishing a common language that organizations use. For example, critical infrastructure sectors have unique terms and concepts that can create challenges with communication. In the Machine Learning, Internet of Things, and software assurance fields, suppliers have evolved unique language with respect to industrial control systems (ICS) that could benefit from efforts to establish a common language and taxonomy.

   B. Benefits of using the CSF include improved risk communications within and between organizations, informed by measurement and metrics. These types of communications are essential to the management of cybersecurity and risk. Expand supporting materials that explain how metrics can be used to support the CSF and organizations using it.

   - Develop suggested metrics or supporting case studies that demonstrate measures on the effects and benefits of CSF implementation.
   - Simplify the development of metrics for cybersecurity improvement. Provide examples for users to consider as they design metrics around cybersecurity.

- Provide example metrics designed for new adopters of the CSF.

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. Challenges that can prevent organizations from using the NIST Cybersecurity Framework or using it more extensively include:
      - resource limitations
      - information-sharing restrictions
      - organizational factors
      - workforce gaps
      - the complexity of the cyber challenge.

   B. Leveraging CSF subcategories may seem obvious until one investigates the supporting references that specify subcategory requirements. This can be challenging. Some references are numerous and point to a wide variety of controls, which can seem counterproductive. The relationship of other references to a given subcategory statement can be unclear. To remedy this, streamline references to better fit the subcategory and, consequently, to make the CSF easier to use.

   C. One challenge has grown substantially since the last revision to the CSF: the ubiquity of machine learning (ML) in many areas of cybersecurity practice, including User and Entity Behavior Analytics (UEBA), traffic filtering, malware analysis, and log event correlation. Because of this, organizations can be reluctant to share the outputs of assessment and investigative tools that use ML, because they are uncertain of the degree of exposure that a model might give to the organization's structure and internal data.

   D. Frequently, there is an organizational divide between those who manage industrial control system (ICS) environments and those who manage traditional IT environments. Key among the many reasons for this is that originally ICS environments were not based upon traditional IT systems, and commonly included custom vendor-specific hardware, software, and / or communications protocols. In addition, ICS environments justifiably rely heavily on availability, which is not always the primary goal of IT systems with respect to IT environments and the confidentiality, integrity and availability (CIA) triad. Finally, management of ICS environments traditionally lies within the Operations or Engineering group while IT is part of a back-office function under the Chief Information Officer. This creates a gulf that is exacerbated by two factors: the technological convergence of the underlying platforms for these environments, and the growing need for bidirectional communications among them.

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.

A. The lowest Framework Implementation Tier that references "senior cybersecurity [...] executives" is Tier 3: Repeatable. The CSF needs a recommendation for the existence of such positions in critical infrastructure organizations and a set of roles for them. This may be most appropriate within ID.GV as an extension to ID.GV-2, or as a stand-alone item. Create such a role, with equal standing to C-suite leaders, for critical infrastructure organizations.

B. Because organizations use tiering concepts widely, explore the use of an approach that considers process management or maturity more extensively. This approach should recognize that the needs of an organization determine the appropriate level of process management. For example, smaller organizations may not require the same level of process management as larger ones.

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.

   Changing the CSF structure may cause problems for organizations that are using the existing structure. This is not a reason *not* to improve CSF, but changes to it should take into account how changes may have an impact on the CSF and offer an appropriate transition.

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

   A. It would be helpful to provide additional case study-oriented information on the use of the 2018 version of the CSF, including value that the addition of access content, supply chain, and tier guidance bring.

   B. Streamlining and/or reordering subcategories will improve the CSF. The order of the subcategories matters in an assessment for the CSF, because there must be an intuitive flow to the assessment questions. For example, PR.AC-1 states "Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes" and PR.AC-6 states "Identities are proofed and bound to credentials and asserted in interactions." It makes sense to group these together, possibly as PR.AC-1 and PR.AC-2, instead of separating them by four other subcategories. When performing an assessment, it is more efficient to ask all related questions in one grouping, rather than jump from topic to topic.

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.

A. The diverse interpretations of such key terms as resilience, security, and cybersecurity supply chain risk management pose challenges to communication and measurement of cybersecurity risk. The advent of the National Initiative for Improving Cybersecurity in Supply Chains will bring these terms into use in related NIST Publications. It is critical that terminology is clear and understandable throughout all NIST materials and related standards such as ISO and DOD 5000.01.

B. Integrate more closely NIST 800-82 (Guide to Industrial Control Systems Security) and the CSF for manufacturing and critical infrastructure. Because most security principles apply to both IT and OT, it would be useful to develop the CSF into a "one stop shop."

C. Consider methods to tie asset management more effectively into the CSF and related NIST Risk Management Framework (RMF) steps. Large federated organizations may have multiple providers and products. Effective risk management increases in complexity as organizations fail to understand their total inventory of people, information, facility, technology, and third-party provider assets. NIST should provide leadership on more effective means for asset management to consider Software Bill(s) of Materials (SBOMs), asset prioritization, and the means for making strong connections of asset value with organizational risk appetite.

D. Integrating various risk management resources requires care. It can be challenging to parse cyber and risk concepts throughout multiple standards or ways of implementing a risk management process. For example, providing clarity on the RMF content and implementation overlaps with the CSF. Aligning these frameworks would pay large dividends to the practice of cyber and risk management. Organizations struggle to determine which framework(s) to follow and to fund the resources necessary to continue doing so on a regular basis.

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?

Strengthen the mapping of the CSF to the ISO 27000 series. These standards have somewhat different perspectives, and understanding how one maps to the other is not always obvious, even from the references in the CSF. NIST could add additional value to the practice of cybersecurity if it describes how these highly influential standards relate to one another.

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?

   Establish a well understood international strategy for collaborating on cyber and supply chain risk management. The NIST website includes a number of examples of CSF-related international activities, for example, "NIST has been holding regular discussions with many nations and regions, and making noteworthy internationalization progress."[1] It will be broadly useful to expand these global efforts around a clearly articulated strategy for supply chain and, in general, cyber risk management. Supply chain-related risks pose a particular challenge when viewed from an international perspective, e.g., state-sponsored and foreign criminal perpetrators of disruptive cyber activities.

   As referenced above, enhance the mapping of the CSF to the ISO 27000 series to strengthen the international understanding of the CSF. ISO and NIST are different; understanding how one maps to the other is not always obvious even with the references in the CSF. Many organizations outside the United States use ISO extensively and are interested in the CSF perspective on leading practices. A more direct and understandable linkage between the CSF and ISO could support enhanced cybersecurity practices globally.

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.

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,

[1] *Is the Framework being aligned with international cybersecurity initiatives and standards?* Retrieved April 21, 2022 from NIST Cybersecurity Framework website, "Questions and Answers: Framework Basics Questions," https://www.nist.gov/cyberframework/frequently-asked-questions/framework-basics

including software security work stemming from E.O. 14028, to increase trust and assurance in technology products, devices, and services?

No input to provide at this time.

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.

    Include in the CSF a model architecture that describes aspects of the supply chain for a specific critical infrastructure area and identifies the critical nature of certain Subcategories in stages of the supply chain. In the energy sector, for example, Subcategories that are critical when considering electrical power generation and transmission are different from Subcategories when considering the enterprises that transport equipment to power generation and transmission facilities. A vertical Tier alignment throughout a critical domain would make the CSF useful for the planning activities of critical infrastructure organizations. In addition, the CSF should pay attention to how to use tools that incorporate ML, both in sourcing and in their effects on information sharing, as well as call out critical infrastructure needs separately, and with strong language, for certain collections of recommendations

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?

    A. Many do not fully recognize the importance of supply chain and dependency risks on organizations and economies. Supply chain cyber risks stem from many organizational dependencies. These risks are broad, significant, and growing as dependency risks and outsourcing options expand. An adversary's cyber-attack on third parties can undermine important mission capabilities, even when an organization does not explicitly contract with suppliers upon which they are dependent. For example, information technology that includes third-party components and services supports or integrates with virtually all products and services an organization acquires. Practices critical to monitoring and managing these risks are scattered across the organization, resulting in inconsistencies, gaps, and slow response to disruptions.

    To help address the many shared challenges faced by organizations NIST is uniquely positioned to lead efforts to address supply chain and dependency risk. The progress made in strengthening cyber risk capabilities as a result of the unified focus that began in 2013 with the build of the CSF, is a testament to what can be achieved. The areas of

supply chain and dependency risk management where exposures are most material include the following:

- Software's role is growing in products, services, systems and networks, making it a linchpin of cyber exposure. The building of software has evolved to use a more component assembly approach often involving a disparate array of domestic and international suppliers.
- Identifying and documenting third-party software to create a software bill of materials (SBOM) has increasingly come to forefront as a necessary practice. The challenge is to establish an adaptive and effective set of leading practices that are collaboratively utilized.
- Expanded use of outsourced processing and cloud providers introduces new cyber risks. Such suppliers do not have consistent, adequate capabilities or resources in place to manage cyber risk effectively.
- Challenges with delivering secure operational environments for increasingly complex systems of systems managed by a diverse set of suppliers.
- Weak or ad-hoc organizational efforts to manage the cyber risk aspects of acquisition and supplier management pose large and growing risks.
- Supplier performance governance and management is critical to managing risk. Key areas of focus may vary by organization, but should include controls testing, threat management, disruption planning and testing, and oversight of the supplier's suppliers.
- Managing supplier access to organization and enterprise assets requires a high level of scrutiny. Many organizations neither focus on this risk nor have a grasp of leading practices in this area.
- Management of supplier transitions are especially important in systems of systems environments, from the onset of forming a supplier relationship.
- The recognition and management of cyber risks posed by suppliers of infrastructure and government services requires additional attention.
- Weak coordination of disruption planning and response activities (i.e., incident management and service continuity) between and among organizations and their suppliers is pervasive.
- Situational awareness and threat management can be essential to managing today's dynamic threat landscape. Organization often lack threat management capabilities internally, and frequently do not work collaboratively with their suppliers to manage cyber risk.

B. Distinguish an emphasis on cybersecurity concerns for supply chains supporting critical infrastructure from the discussion of risks introduced by the supply chain supporting cybersecurity tools, with respect to both hardware and software. Recent vulnerabilities have drawn attention to the need for risk management in the components of cybersecurity tools. An update to the framework could reduce challenges in adoption by both addressing the cybersecurity supply chain and providing a clear distinction

between this concern and cybersecurity practice in the critical infrastructure supply chain.

C. The application of machine learning models to the supply chain of cybersecurity tools presents novel and difficult-to-evaluate risk. Solutions would be easier to implement if they included guidance for assessing and evaluating cybersecurity tools dependent on components driven by ML models.

D. The ongoing and growing migration to commercial cloud is widespread among both commercial and government organizations. The risks posed by this migration to supplier managed environments merit expanded focus by NIST.

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.

The development of a new and separate framework focused on supply chain risk management could be problematic because:

- The CSF Core is a "set of cybersecurity activities, outcomes, and references"[2]. Focus on the existing CSF core outcomes, in conjunction with appropriate supply chain considerations, could lead to acceptable risk-managed outcomes. Supply chain risk is integral to cybersecurity risk management and should not be treated separately.
- The existing framework allows for an appropriate amount of interpretation. If a new interpretation is added, it raises questions about an endless array of emerging concepts (e.g., zero trust) that may require their own analogous framework. This could lead to unnecessary noise in a world where many frameworks exist, and create additional confusion.

[2] *An Introduction to the Components of the Framework: Framework Core*, Retrieved April 21, 2022 from NIST Cybersecurity Framework website, https://www.nist.gov/cyberframework/online-learning/components-framework