Trellix

We bring security to life.

April 25, 2022

Submitted via email to CSF-SCRM-RFI@nist.gov

Cybersecurity Framework
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

Re: Trellix's comments in response to NIST's Solicitation for Comments on 'RFI: Evaluating and Improving Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management'

Trellix welcomes the opportunity to provide input to the NIST Cybersecurity Framework (CSF) RFI. Trellix is a living security company redefining the future of cybersecurity. Trellix is delivering adaptable, innovative security solutions to organizations around the world. The company's open and native extended detection and response (XDR) platform provides a holistic ecosystem that consolidates security products into an interconnected, constantly communicating platform that's always learning and adapting to new and evolving threats. Forged by the combination of the highly skilled McAfee Enterprise and FireEye teams, Trellix is dedicated to transforming the way organizations think about digital security by delivering best-in-class technology and expertise. Today's dynamic world demands a holistic, integrated ecosystem and a cloud-first approach allowing all security products to work in unison. By harnessing the power of machine learning and automation to unlock insights and streamline workflows, Trellix helps organizations stay one step ahead of adversaries, adapt to new threats, and accelerate detection and correction throughout the entire cyber defense lifecycle. Trellix's cybersecurity and threat experts, along with an extensive global partner ecosystem, are accelerating security technology innovation. Trellix is empowering over 40,000 business and government customer organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations.

Our response includes answers to specific questions asked, as well as general comments. Please note, our use of "Cybersecurity Framework", "CSF" and "Framework" in our comments below are used interchangeably to reference the NIST Cybersecurity Framework.

Our developmental principles for guiding the creation of the CSF 2:

- The Framework needs to continue to be as widely applicable and as flexible to use as possible.
- We need to ensure the CSF does not become the kitchen sink of ideas for improving security but remains focused on being the foundational document for fostering organizational cyber risk management.
- We need to review the critical items any organization needs to have as a core part of their cyber risk management program improvement process. This will help identify what we are missing.
- Aspects of the Core need to be addressed. For example, Tiers needs to be refocused to be more useful than the basic model put in place in the 1.x CSF versions

6220 American Center Drive,
San Jose, CA 95002
888.847.8766
trellix.com

- Explanation and true understanding of what a Target Profile is, and its value to the organization is critical to making the Framework process easier to understand and use.
- The Cybersecurity Framework is not just for enterprise risk evaluation. It can be applicable for project, service and even product development risk evaluations. Additional considerations of how to tailor the framework for project evaluation vs enterprise evaluation are needed.
- The Framework needs to define a clear process for future incremental updates.
- International considerations and outreach are critical for aligning and improving cybersecurity globally. All governments and critical infrastructure outside the U.S. should be actively encouraged to participate in the CSF 2 development process.
- Every organization develops software and thus the CSF should incorporate how an organization should be approaching secure software development and intellectual property protections, not just for commercial software, but for internal corporate needs.
- It is important the development of NIST CSF 2.0 follow the same general process that occurred in the 1.0 version of the CSF.
- The CSF should focus on international standards as base informative references wherever possible. This includes international standards that are not currently incorporated but should be. A review is needed to assure the appropriate and applicable standards are referenced.
- Integrating software development, supply chain and metrics into the CSF should be done within the existing five top-level functions. While new categories and subcategories are expected and encouraged, NIST should avoid adding new top level functions as the existing Framework has become a standard language for the cyber risk management community.
- Finally, ensure the NIST Cybersecurity Framework remains focused on being the tool that enables organizations to build and refine their own organizational cyber risk management programs. Cyber risk management must be integrated into and complement the other established corporate risk management domains.

Comments Requested in the RFI:

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.***

   We believe the CSF has been highly successful in becoming the focused reference framework for cyber risk management processes and procedures within organizations that have embraced it. Prior to the release of the CSF in 2014, organizations were largely focused on regulatory compliance and not on their actual cybersecurity risk posture. The CSF had a profound impact on reorienting and transitioning organizational thinking towards cyber risk management.

   The language of the five functions allowed conversations to be had at all levels of the organization, from the Board Room to the Security and Network Operations Centers, and throughout corporate management. It provided a common language that has enabled highly complex subjects and the problems and funding surrounding them, to be expressed

in a way that could be understood at all levels of an organisation.

The CSF, rightly, did not dictate an organization change how they previously did things in order to use the CSF, but allowed organizations to map their current processes into the CSF via the highly useful informative references focused on international, and national standards and industry best practices.

The CSF Core (categories and subcategories) allowed organizations to see where there may be areas that needed to be addressed but were previously not considered nor implemented.

The CSF also helped to facilitate conversations that most organizations had never had. ***What is the level of cyber risk that my organization is willing to accept?*** Sounds like a simple question but organizations large and small had never had that set of discussions. It should be understood that *Cyber Risk Management* is just another form of corporate risk management. Businesses are highly competent at many aspects of "Corporate Risk Management," such as financial risks, environmental risks to corporate facilities, competitive risks, physical risks, dependency risks, risks to shareholders, etc. What needs to occur is the understanding that Cyber Risk Management should be and must be incorporated into any corporate risk management governance process.

Over the past eight years since its initial release, the Cybersecurity Framework has fostered cyber risk management's integration into existing corporate risk management programs, and all without excessive costs. This has resulted in better organization visibility into where, how and at what level resources should be applied. When an organizational CSF assessment is done on a consistent periodic basis, the organization can see (or not) the improvements being made while enabling better agility in determining how to address the evolving nature of cyber risks to the organization.

We believe the Cybersecurity Framework has been extremely useful as a cyber risk management tool allowing organizations who use it to incorporate cyber risk management more successfully into their everyday operations.

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?**

As previously stated, communications within organizations that use the Cybersecurity Framework are much improved. The CSF also improved communications between organizations that are either supplying or being supplied products and services to others. It provided a foundational mindset that allows for a better understanding of what is being discussed between organizations. Shortly after the initial publication of the CSF in 2014, corporate Suppliers Security Guides at multiple organizations were modified to

incorporate statements showing the intent to use the Cybersecurity Framework moving forward as a means to communicate cyber risk management considerations.

The ways in which the Framework has improved cyber risk management have been widely recognized and documented internationally. In fact, the NIST Cybersecurity Framework home on the NIST.gov site[1] has posted a good deal of those examples and resources.

As to the question of "*What might be relevant metrics for improvements to cybersecurity.*.", this is a *topic that needs to be actively discussed as a CSF developmental workshop topic*. We have seen a wide variety of means to measure the results of the Framework assessment process. It is our observation that organizations actually create their own means to do so initially as a part of getting started. This is a complicating factor in understanding the Framework assessment process and slows the initial integration. Once a means for measuring and assessing is documented and understood, the process begins. Often what works for one specific initial assessment, may not be as useful in trying to compare multiple assessments done over time. This results in the metrics having to be enhanced or augmented to ensure that trend information can be readily visualized, understood and utilized. It is the trend information that is most valuable. Yes, seeing where an organization actually is compared to its target "acceptable level of risk" profile is highly useful for a point in time evaluation. However, cyber risk management is a process of continuous improvement, identifying, evaluating and mitigating risk over time. Being able to compare the multiple assessment results in a consistent fashion is critical to seeing if the organization is going in the right direction by reducing cyber risk. Any means for providing guidance as to how to use metrics needs to address the "point-in-time" CSF assessment and also how to properly compare results over a relevant set of point-in-time results.

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).**

Educational guidance on how to use the Cybersecurity Framework is not as extensive and useful as it needs to be. Regardless of the size of the organizations, the CSF can be used to evaluate where the organization stands from a cyber risk perspective. However, organizations still require support and guidance at the outset so they can better understand what they expect to get out of it, figure a way to institutionalize consistent periodic assessments and continue to have support for it across the organization levels. Just understanding where and how to start can be daunting.

The biggest hurdles for incorporating the CSF into the organization are those that are encountered initially. Once there is some understanding and experience working with it, the process becomes much easier during subsequent assessments.

[1] NIST Cybersecurity Framework Home Page: https://www.nist.gov/cyberframework

Organizations need to train internal company assessment staff, have a means for scoring and the needed supporting assessment tools (spreadsheets, documentation, etc.) in place in order to undertake an assessment. Often this takes a 'CSF Champion' to foster the initial adoption of the effort internally and that can be a barrier if there is not one available. Historically, being able to sell the value of using the CSF process to management and executive management is time consuming in itself.

Additionally, organizations today are using the CSF for more than just a corporate-wide cybersecurity risk assessment tool. Companies have adapted the CSF for project related cyber risk evaluations and for deployment of new services or products. This has become possible as organizations become more experienced with using the CSF and the cyber risk management mindset.

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.**

Tiers:
In previous comments made, we have indicated that the Tiers are one area that needs serious focus. More concrete guidance needs to be provided to assessors as to how to utilize the Tiers in evaluating an organization's categories and subcategories. The CSF 1.x looks at Tiers in the three areas of Risk Management Process, Integrated Risk Management Program, and External Participation. While simple and useful at a high level, the CSF should modify the definition of Tiers to be based on the more traditional breakdown of People, Process, Technology and Ecosystem. This approach has some interesting scoring and metric potentials.

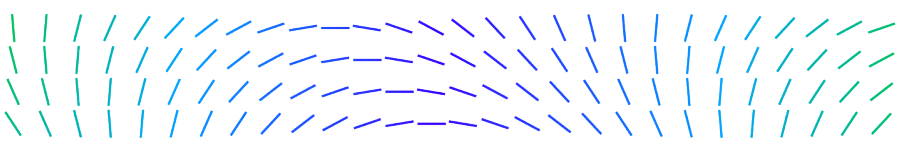
The following table depicts a customization that was done by Intel as a part of their initial implementation of the Cybersecurity Framework 1.0 shortly after the CSF was initially published. This table was taken from the Intel Whitepaper "The Cybersecurity Framework in Action: An Intel Use Case"[2]. The author of these comments was also one of the co-authors of the Intel whitepaper that documented our initial efforts at using the CSF. Even eight years later, the belief is that having a bit more granularity in the Tier definitions makes their use easier and more consistent. While we are not suggesting NIST take this customized set of Tier definitions and use them directly, we are indicating that the approach of using people, process, technology and ecosystem is more useful and relates more to the cyber risk management focus the CSF is addressing. It allows for interesting potential means of scoring based on any of the four main areas as well, potentially making the Tiers an even more valuable means for scoring.

[2] https://www.intel.com/content/dam/www/public/us/en/documents/solution-briefs/cybersecurity-framework-in-action-use-case-brief.pdf

FOCUS AREA	TIER 1 PARTIAL	TIER 2 RISK INFORMED	TIER 3 REPEATABLE	TIER 4 ADAPTIVE
People	• Cybersecurity professionals (staff) and the general employee population have had little to no cybersecurity-related training. • The staff has a limited or nonexistent training pipeline. • Security awareness is limited. • Employees have little or no awareness of company security resources and escalation paths.	• The staff and employees have received cybersecurity-related training. • The staff has a training pipeline. • There is an awareness of cybersecurity risk at the organizational level. • Employees have a general awareness of security and company security resources and escalation paths.	• The staff possesses the knowledge and skills to perform their appointed roles and responsibilities. • Employees should receive regular cybersecurity-related training and briefings. • The staff has a robust training pipeline, including internal and external security conferences or training opportunities. • Organization and business units have a security champion or dedicated security staff.	• The staff's knowledge and skills are regularly reviewed for currency and applicability and new skills, and knowledge needs are identified and addressed. • Employees receive regular cybersecurity-related training and briefings on relevant and emerging security topics. • The staff has a robust training pipeline and routinely attend internal and external security conferences or training opportunities.
Process	• A risk management process has not been formalized; risks are managed in a reactive, ad hoc manner. • Business decisions and prioritization are not factored into risk and threat assessments. • Risk and threat information is not communicated to internal stakeholders.	• Prioritization of cybersecurity activities is informed by organizational risk objectives, the threat environment, or mission requirements. • Risk-informed, management-approved processes and procedures are defined and implemented, and the staff has adequate resources to perform its cybersecurity duties. • Cybersecurity information is shared within the organization on an informal basis. • Management has approved the risk management practices, but these practices may not have been established as organizational-wide policy.	• Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business or mission requirements and a changing threat and technology landscape. • Consistent risk management practices are formally approved and expressed as policy, and there is an organization-wide approach to manage cybersecurity risk. • Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed.	• Cybersecurity risk management is an integral part of the organizational culture. • The organization actively adapts to a changing cybersecurity landscape, evolving and sophisticated threats, predictive indicators, and lessons learned from previous events in a timely manner. • The organization continually incorporates advanced cybersecurity technologies and practices. • There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures.
Technology	• Tools to help manage cybersecurity risk are not deployed, not supported, or insufficient to address risks. • Tools may be in place but are not adequately tuned or maintained. • Technology deployed lags current threats. • Tool deployment may not adequately cover risk areas.	• Tools are deployed and supported to address identified risks. • The tools in deployment are tuned and maintained when resources are available. • The technology deployed, for the most part, keeps pace with current threats. • Tool coverage of the risk area is complete when deployed.	• Metrics are used to evaluate the usefulness and effectiveness of the deployed tools. • The tools in deployment are routinely tuned and maintained. • The technology deployed keeps pace with current and emerging threats. • Tool coverage of the risk area is complete and updated as changes are recognized.	• The tools deployed in the environment are regularly reviewed for effectiveness and coverage against changes in the threat environment and internal ecosystem. • The tools and technology deployed anticipate emerging threats.
Ecosystem	• The organization does not understand its role in the larger ecosystem or act accordingly. • The organization does not have processes in place to participate in or collaborate with external organizations on cybersecurity issues.	• The organization knows its role in the larger ecosystem but has not formalized its capabilities to interact and share information externally. • The organization may participate in or collaborate with external organizations on cybersecurity issues on an ad hoc basis.	• The organization understands its ecosystem dependencies and partners and can act accordingly when it receives information from these partners.	• The organization manages risk and actively shares information with partners to ensure that accurate, current information improves ecosystem cybersecurity before events occur.

Profiles:

The description of Profiles, what they are and how to use them needs better explanations. The CSF documentation needs to explain more precisely what the profiles are and the flexibility surrounding them. It is not clear what a Target profile really is. The CSF describes the Target Profile as the "to be" state. We believe this description is questionable at best. In actuality, the Target Profile is documenting the "Acceptable



6220 American Center Drive,
San Jose, CA 95002
888.847.8766
trellix.com

Level of Risk" an organization can tolerate. If a Target Profile is to be useful, it needs to be developed as an outcome of conversations on what level of risk the organization's leadership is willing to accept and manage to. These conversations need to be at the highest levels of the organization and the outcome, or Target Profile, needs to have the approval / signoff of executive management. Cyber risk management directions, funding and approvals need to have that level of backing since risk management is a corporate governance responsibility. In one case, we have heard of the Target Profile being used as a briefing tool for the corporate Board. It was the foundation for the presentation depicting how the leadership team perceived the level of threats and cyber risk to the organization.

It also should be understood the Target profile needs to be reviewed and re-approved on an established periodic basis. Threats are not static. The threats to the organization change over time. To be useful, the Target profile needs to evolve as well. This allows corporate cyber risk management operations staff to have real corporate directions and have a better understanding of the evolving threat landscape in order to properly protect the organization.

Integrity of the assessment process
The following are the Steps specified in Section 3.2 of the CSF.

Establishing or Improving a Cybersecurity Program:

Step 1: Prioritize and Scope
Step 2: Orient
Step 3: Create a Current Profile
Step 4: Conduct a Risk Assessment
Step 5: Create a Target Profile
Step 6: Determine, Analyze, and Prioritize Gaps
Step 7: Implement Action Plan

This is one area where the size of the organization can impact our comments below. We believe most organizations should consider intentionally separating those individuals who created the Target Profile from the actual Assessment team. We do this so as not to bias the Assessment SMEs evaluation with what we were targeting to achieve.

As previously mentioned, the Target profile should be created as an outcome of discussions with executive management on what is an acceptable level of organization risk. We believe and encourage organizations using the CSF as a cyber risk assessment tool to separate the team that creates the Target Profile from the team doing the actual assessment using the agreed to categories and subcategories. The Assessment team should not be aware of the specifics of target profile until the assessed results are compiled. We believe this approach is essential to the integrity of the overall process and should be mentioned in the Framework process documentation. We believe this should be called out in section 3.2, Establishing or Improving a Cybersecurity Program. This

separation should be continued in subsequent years as the organization reviews and updates their Target Profile to accurately reflect their current organizational level of acceptable risk. As documented today, we believe that creating a Target Profile after knowing the results of the Current Profile is similar to some educators "teaching the test".

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.**

   Making wholesale changes to the CSF as insinuated by this question, is not recommended. Depending on the level of changes, it could vastly complicate an organizations ability to see trends that may be emerging if the results are too radically different. We believe there is no need to make radical changes to the structure of the CSF.

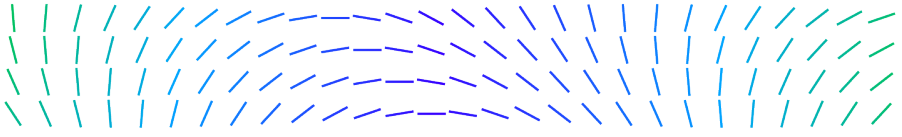
   We believe a thorough review of what is missing from an organizational risk perspective -- for example, cyber supply chain needs and secure software development processes – is necessary. Then using the existing CSF Core component architecture, add the additional categories, subcategories and informative references to incorporate the needed additions into the Framework. It does not appear, at this point, there is a need for a new top level Function. We believe the structure itself is sound and adaptable to what is needed to properly update the Framework. Our earlier recommendation about modifying the Tier definitions is simply an extension and we believe it would not impact any form of backward compatibility from CSF 1.x usage.

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

   Before expanding the CSF to incorporate secure software development, and supply chain security issues, it is important to note the CSF is in need of more structured documentation describing how organizations can create a cyber risk management program or fit the CSF into an existing cyber risk program. The value of the CSF is still waiting to be tapped as a true foundation for cyber risk management.

   Granted, as we have mentioned, the CSF has had a great influence on the landscape, but in our opinion, it is falling short of making it easier for organizations to start using it. While brevity was important in the 1.x versions, it is not beneficial to continue to have to make all organizations figure out how to get started. That is not saying all the needed information must be included directly in the CSF specification itself. While the existing text does need more information, much more in-depth treatments of a topic could be created as a separate document and referenced from within the CSF specification. Additionally, more clarity is needed as to what various sector, technology or threat Profiles exist and where they fit into the overall CSF Risk Management architecture.

Relationship of the NIST Cybersecurity Framework to other Risk Management Resources



6220 American Center Drive,
San Jose, CA 95002
888.847.8766
trellix.com

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.**

    There are two steps needed to assure proper integration of these NIST resources into the Cybersecurity Framework structure.
    - Each of the resources listed address people, processes, controls or technology. It needs to be investigated if categories and subcategories exist where these can be integrated. In many cases new categories and subcategories may be needed in order to properly incorporate these resources and references into the Framework structure. The CSF lends itself to be adapted and expanded in this fashion. The current structure should be used wherever possible.
    - Each of the resources identified in the question are informative references and they should be listed in the proper subcategories as such.

    This approach allows the topics are incorporated into the Framework in a manner consistent with the initial design and architecture of the Framework. This actually should be a straightforward exercise. Sometimes it is better to look at the simple ways to accomplish things instead of the complex. Using the power of the existing Cybersecurity Framework architecture to our advantage benefits all and causes less potential negative impacts to the CSF global usage.

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?**

    This is one area of discussion that is needed during the CSF 2 developmental workshops. Non-NIST Frameworks or approaches have been incorporated into the Framework from Day 1. Informative references enabled organizations to map their use of these non-NIST frameworks and controls into the CSF. It was done in this manner to assure organizations could identify what they were already doing and what still needed to be addressed. The question in this area is really not clear and should be a topic for a developmental

workshop session. The work being done in ISO/IEC efforts is for the most part, being accomplished by people that actively participated in the initial NIST CSF efforts.

We believe the CSF should not incorporate U.S. government specific guidance. This has been something we have heard internationally. "The NIST CSF is a US effort, documenting US needs and not something we can use." Not only is this incorrect, but it does nothing to assist in aligning international cybersecurity operational norms and regulations. Global companies need international alignment to facilitate efficient use of corporate resources. Where we can avoid dealing with non-aligned regulations and approaches to cybersecurity, we should. It can be costly and potentially open up attack vectors for adversarial exploitation. Besides, last checked, NIST was an agency of the Commerce Department whose ***mission of the Department is to create the conditions for economic growth and opportunity for all communities.*** (Sorry, could not resist.)

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?**

   Understanding why the adaptation or changes were made is critically important. There may be real positive reasons from which the CSF could benefit. When the CSF was initially developed, it was done with little participation and visibility past our borders. Cybersecurity is a global problem, and many internationally may have issues that we were not either aware of or concerned with at the time.

   We need to enssure we incorporate as much international participation in the Framework as possible. That means reaching out to non-US governments and organizations to encourage and incentivize them to participate in the developmental workshops and provide comments and feedback during the overall process. The diversity of thought in having global participation in the development of the Framework will create a better outcome for all.

   Additionally, after the release of both versions of the CSF, NIST encouraged those in the private sector who have been actively involved with the development of the CSF to reach out to their international contacts and customers to help advocate for the use and adoption of the Framework. Our company gave in-country presentations, having had discussions in Japan, Australia and France with government officials and business leadership on the benefits of the Cybersecurity Framework. NIST should consider encouraging this approach once again.

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

This is a mapping exercise for the documents listed above. Additionally, updates are needed to the existing 1.x references to assure they are current with the later versions of the referenced standards and best practice documents. This is something that could be done as a preparation for a developmental workshop. NIST could consider establishing temporary working groups focused on nothing except mapping identified standards document to the existing and emerging subcategories.

One area recommended for reference improvement in the past has to do with RS.AN-5, focused on Coordinated Vulnerability Disclosure (CVD). The existing informative references identified do not relate directly to coordinated vulnerability disclosure and handling. Two international standards that are widely used as the basis for CVD process globally are ISO/IEC 29147[3] and ISO/IEC 30111[4]. Neither of these are currently referenced in the CSF and should be. It is our recommendation the CSF use the most applicable and appropriate references, so CSF users develop recognized CVD processes aligned with international standards and best practices. In the case of coordinated vulnerability and handing (RS.AN-5), these two references must be included.

11. **National Initiative for Improving Cybersecurity in Supply Chains (NIICS). What arethe 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 EO 14028, to increase trust and assurance in technology products, devices, and services?**

We encourage NIST to take a more forward-looking and inclusive view of the Administration's supply chain security work-streams and how best to update these. Supply chain security has been a very active topic across multiple agencies and industry efforts. Focusing only on the work done at NIST robs NIST and the CSF community of all the great work that has occurred within other efforts. It would be beneficial to identify the supply chain security initiatives that have occurred throughout the federal government. Those public-private partnerships produced reports and recommendations that should be considered and at a minimum, be used to inform the NIICS efforts. Questions 11 – 14 should be asked again in relation to the previously existing supply chain security reports and recommendations from those

[3] ISO/IEC 29147:2018, Information technology – Security techniques – Vulnerability disclosure, International Standards Organization, Oct. 2018, https://www.iso.org/standard/72311.html.

[4] ISO/IEC 30111:2019, Information technology – Security techniques – Vulnerability handling processes, International Standards Organization, Oct. 2019, https://www.iso.org/standard/69725.html.

earlier efforts. The following three questions should be the basis for one on the upcoming NIST CSF 2 development workshops.

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.**

    We propose to defer this question to a NIST CSF 2.0 workshop.

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?**

    We propose to defer this question to a NIST CSF 2.0 workshop.

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.**

    We propose to defer this question to a NIST CSF 2.0 workshop.

Additional Comments

CSF 2.0 Development Process:
It is critically important the development of a NIST CSF 2.x follow the same general process that occurred in the 1.0 versions of the CSF. One of the smartest things NIST did initially during the Cybersecurity Framework 1.0 development was to create an iterative process, taking the development workshops on the road. Having workshops in various parts of the U.S. allowed asset owner/operators, asset managers and others not familiar with the Washington DC Beltway processes, to actively participate when NIST came to their local community. This brought a great deal of experience to the table and greatly enhanced the development of the CSF. This one decision by NIST created a better overall outcome. The CSF 1.1 process was more streamlined and not as impactful. If the goal of this current effort is to create a 2.0 version of the Framework, the model used initially to develop 1.0 would be most beneficial to producing a better outcome.

The approach taken with CSF 1.0 also had some positive social side effects of getting people to buy in and take ownership of the Cybersecurity Framework development for their organization. When the CSF published on February 12, 2014, it already had a great deal of support from those who had been active participants in its development. We believe that those 3000+ people who actively contributed to the CSF's initial development became the first advocates for its adoption. NIST should use the same process of having workshops on the road across the US and potentially in other countries.

International participation:
International participation is vital if the CSF is going to have the global impact we all hope it does. NIST should consider holding a workshop internationally. This will have multiple benefits. First it will show that the CSF development process is open, transparent and not just a U.S. effort. It will get people who participate familiar with the CSF, its usage and have real input that will most likely help to produce a better, more aligned outcome. NIST should consider presenting and solicitating participation in international forums such as the US/EU Technology and Trade Council and the Quadrilateral Security Dialogue (QSD).

Encouraging State Government Participation:
Participation is key to creating a better outcome. While there should be a great deal of encouragement for international participation, it is important we also focus on encouraging U.S. state governments to actively contribute to the CSF 2.0 development. NIST, along with the Cybersecurity and Infrastructure Security Agency (CISA) should look at ways of incentivizing state governments to attend and contribute. This benefits the effort by bringing a different set of perspectives. It also would have the post-effort effect of the participating states wanting to take what was developed / learned back to their home state for use and adoption. As stated earlier, sometimes it takes a "CSF Champion" to foster the efforts in their organization.

Work within the Cybersecurity Framework Architecture:
The initial CSF Core architecture was highly effective at enabling organizations to use and modify it without breaking it. The flexibility provided allowed the CSF to be used in ways not initially envisioned, such as product and service evaluations in addition to corporate security posture assessments. While there are some major enhancements needed, integrating software development, supply chain and metrics into the CSF should be done within the existing five functions. While new categories and subcategories are expected, NIST should make all efforts to not add to the top level functions.

Possible CSF Workshop Topic Areas

While the RFI process will garner a great set of input, many of the areas, where more information is desired, will result only from the active conversations occurring during development workshops. Suggested below are a few items we would like to see discussed during the NIST CSF 2 developmental workshops.

- Utilizing non-NIST frameworks or approaches in conjunction with the NIST Cybersecurity Framework. Are there commonalities or conflicts? Are they different?

- How to integrate supply chain risk management more holistically in a way consistent for all organizations? Verifiable supply chain artifacts? Questions 11-14 should be used as the basis for a targeted workshop on secure supply chain risk management.
- *CSF Measurement Mechanisms and Use cases*
    - *What might be relevant metrics for improvements to cybersecurity* ?
    - Scoring CSF Point-in-time assessments
    - Measuring and visualizing trends of multiple periodic CSF assessment results
    - Sector profile results comparisons
- Incorporating Secure Software Development Practices into the CSF
    - Commercial Software considerations and artifacts
    - Internally developed software
- How do emerging threats, vulnerabilities and cyber threat sharing impact the Framework?
- Dealing with technology innovation (IoT, IT/OT, cloud and mobile) and their associated impact to the CSF
- What areas are missing from the CSF that all organizations must incorporate into their cyber risk considerations?

Summary

The NIST Cybersecurity Framework has been by anyone's measure, a highly successful effort to make a difference. Over the last few years, the Framework has successfully helped to change the dialog and organizational focus from "compliance" to "risk management" within a large portion of U.S. and global organizations. This is an extremely positive trend. As we look to incorporate Secure Software Development, Secure Supply Chain Risk Management, develop metrics to make the CSF more precise, more measurable and generally make the CSF a more useful tool, we need to ensure the focus of the CSF remains as a tool for organizations to be able to build and improve their cyber risk management programs, processes and outcomes.

Thank you again for allowing us the opportunity to provide our comments on the Cybersecurity Framework 2.0 RFI. The Framework commendably represents an effort to solve the complex problem of protecting ourselves from evolving cybersecurity threats in a way that harnesses private sector innovation while addressing the cybersecurity needs of governments, businesses and citizens. The focus on reviewing, understanding, and improving organizational cyber security protection programs is a positive change from where organizational focus was in the not too distant past.

Trellix is committed to continuing to partner with NIST on public-private initiatives to improve cybersecurity and cyber risk management. We look forward to our continued collaboration improving the NIST Cybersecurity Framework and cyber risk management capabilities.

6220 American Center Drive,
San Jose, CA 95002
888.847.8766
trellix.com